550 SEP 2 4 1988

247

C 13.10: 500-158

U.S. Department of Commerce

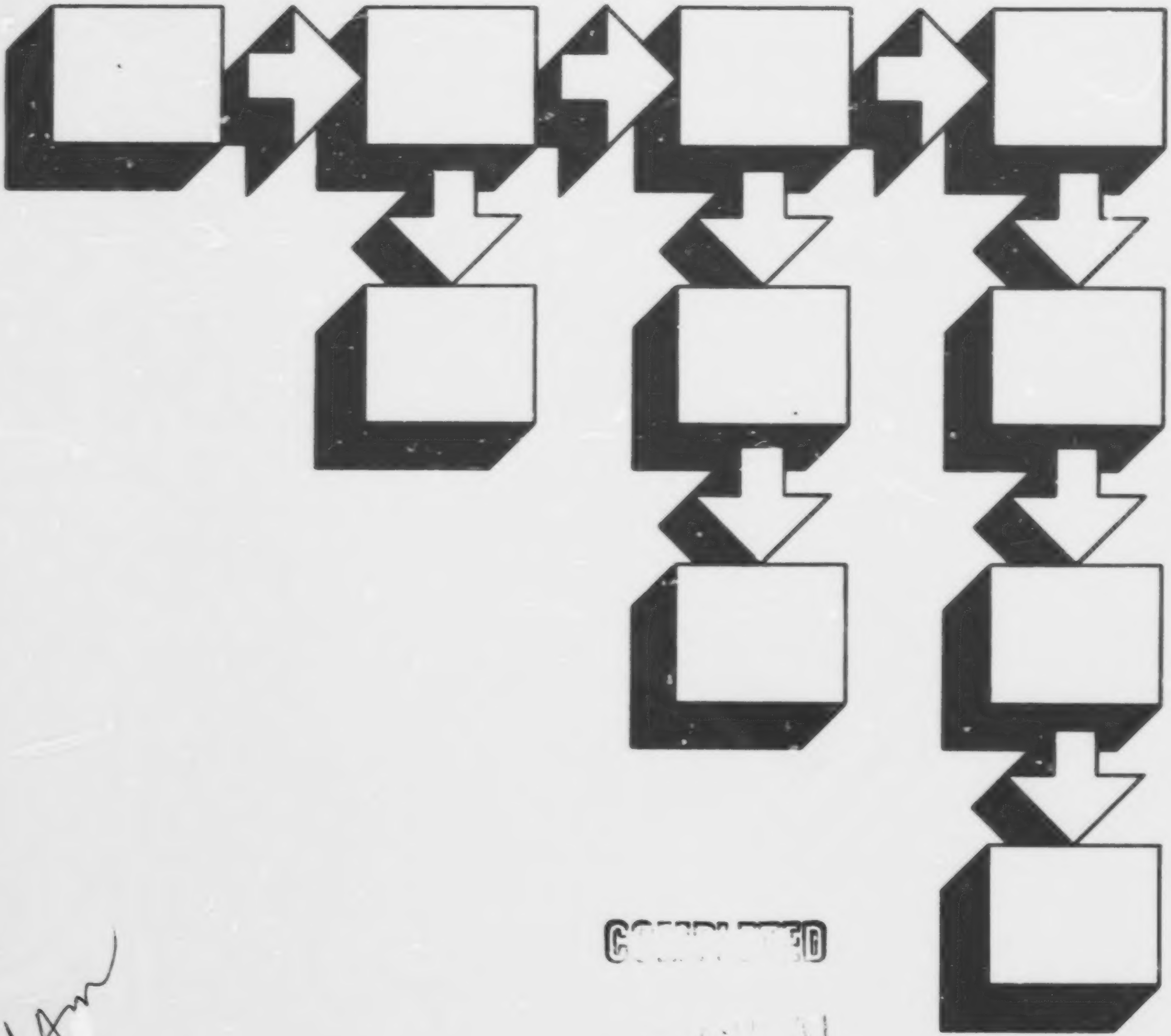
National Bureau
of Standards

Computer Science and Technology

NBS Special Publication 500-158

Accuracy, Integrity, and Security in Computerized Vote-Tallying

Roy G. Saltman



COMPLETED

ORIGINAL

nel/Am

The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NBS work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the Institute for Computer Sciences and Technology, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Computing and Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

The Institute for Computer Sciences and Technology

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Bureau-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

---

[1] Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.

[2] Some divisions within the center are located at Boulder, CO 80303.

[3] Located at Boulder, CO, with some elements at Gaithersburg, MD.

Computer Science and Technology

NBS Special Publication 500-158

Accuracy, Integrity, and Security in Computerized Vote-Tallying

Roy G. Saltman

Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

Sponsored by:

John and Mary R. Markle Foundation
75 Rockefeller Plaza, Suite 1800
New York, NY 10019-6908

August 1988

U.S. DEPARTMENT OF COMMERCE
C. William Verity, Secretary

National Bureau of Standards
Ernest Ambler, Director

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the governmental, academic, and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 88-600573
National Bureau of Standards Special Publication 500-158
Natl. Bur. Stand. (U.S.), Spec. Publ. 500-158, 143 pages (Aug. 1988)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1988

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING

Roy G. Saltman

Recommendations are provided to promote accuracy, integrity, and security in computerized vote-tallying, and to improve confidence in the results produced. The recommendations respond to identified problems, and concern software, hardware, operational procedures, and institutional changes.

It is proposed that the concept of internal control, almost universally used to protect operations that produce priced goods or services, be adapted to vote-tallying, a non-priced service. For software, recommendations concern certification, assurance of logical correctness, and protection against contamination by hidden code. For hardware, recommendations concern accuracy of ballot reading, and design and certification of vote-tallying systems that do not use ballots. Improved pre-election testing and partial manual recounting of ballots are recommended operational procedures.

Some recent significant events concerning computerized vote-tallying are reported. These events include development of performance specifications, publication of a series of New York Times articles, and activities in Texas leading to passage of a revised statute on electronic voting systems. Relative vulnerabilities of different types of vote-tallying systems, i.e., punch card, mark-sense, and direct recording electronic, are discussed. Certain recent elections in which difficulties occurred are reviewed, and categories of failures are highlighted.

Key words: accuracy; computer; election; integrity; internal control; public administration; security; vote-tallying.

ACKNOWLEDGEMENTS

The author wishes to acknowledge assistance received from those individuals who provided documentation of election difficulties, reviewed drafts of this report, or otherwise gave of their time and ideas. These persons include Penelope Bonsall, Director, FEC Clearinghouse; Robert Boram, Director of Engineering, R.F.Shoup corp.; Kimball Brace, President, Election Data Services, Inc.; David Burnham, journalist, Washington, DC; David Clampitt, Oklahoma City, Oklahoma; Terry Elkins, Dallas, Texas; Curtis Fielder, DFM Associates; Emmett Fremaux, Jr., Executive Director, DC Board of Elections and Ethics; Marie Garber, formerly Administrator, Maryland State Administrative Board of Election Laws; Paul Goldy, President, and Jacob Merriwether, Vice President, International Technology Group; Russ Harlan, Assistant Registrar of Voters, Placer County, California; Michael Harty, formerly Director of Voting Systems and Standards, Illinois State Board of Elections; Ralph Heikkila, Assistant Registrar-Recorder, Los Angeles County; Lance Hoffman, professor of computer science, George Washington University; Michael Lavelle, formerly Chairman, Chicago Board of Election Commissioners; Robert Lemens, formerly Assistant Attorney General, State of Texas; David Link, Dean, Notre Dame Law School; Conny McCormack, formerly Director of Elections, Dallas County, Texas; John Medcalf, President, VOTEC; Robert Naegele, President, Granite Creek Technology; Tod Rapp, President, Triad GSI; Jim Riggs, formerly Director of Elections, Maricopa County, Arizona; Deborah Seiler, Chief, Elections and Political Reform Division, State of California; Larry Slesinger, formerly Program Officer, John and Mary R. Markle Foundation; Richard Smolka, editor, Election Administration Reports; David Stutsman, attorney, Elkhart, Indiana; Robert Tyre, Executive Vice President, Business Records Corporation; Malin VanAntwerp, Project Director, ECRI, Plymouth Meeting, PA; Thomas Van de Bussche, Director of Data Processing, Carroll County, Maryland; Douglas Webb, Senior Consultant, SRI International; Britain Williams, Chief, Computer Technology and Applications Division, Georgia Tech Research Institute; Jackie Winchester, Supervisor of Elections, Palm Beach County, Florida.

Regardless of assistance received, the author accepts full responsibility for the content of this report.

Roy G. Saltman

TABLE OF CONTENTS

1. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS 1

1.1 Problems Of Computerized Vote-Tallying 1
1.2 Government Responsibilities. 1
1.3 Implementation Of An Internal Control Function . . . 2
1.4 FEC Clearinghouse Specifications 3
1.5 Revised Texas Statute On Electronic Voting Systems . 3
1.6 Recommendations On Software. 3
    1.6.1 Certification 3
    1.6.2 Integrity and Logical Correctness 4
    1.6.3 Dedicated Software Use and Dedicated Operation 4
1.7 Recommendations On Hardware. 5
    1.7.1 Accuracy of Ballot Reading. 5
    1.7.2 Elimination of Pre-Scored Punch Card Ballots. 5
    1.7.3 Counting of Rejected Ballots. 5
    1.7.4 Required Research 5
    1.7.5 Design of Direct Recording Electronic (DRE) Machines. 6
    1.7.6 Certification of DRE Data Entry Logic 6
1.8 Recommendations On Operational Procedures. 6
    1.8.1 Pre-Election Checkout 6
    1.8.2 Audit Trails. 7
    1.8.3 Complete Data From Split Precincts. 7
    1.8.4 Access Controls 7
    1.8.5 Application Internal Controls for Ballot-Tallying Systems. 7
    1.8.6 Application Internal Controls for DRE Systems 7
1.9 Relative Vulnerabilities Of Different System Types . 8
1.10 Review Of Recent Difficulties In Computerized Vote-Tallying. 8
1.11 Future Vote-Tallying Systems 8

2. BACKGROUND, AND RECENT SIGNIFICANT EVENTS. 9

2.1 Accuracy, Integrity, And Security. 9
2.2 ICST's 1974/1975 Project On Computerized Voting. . . 10
2.3 Some Pertinent Technological Changes Since 1975. . . 10
2.4 Development Of Standards For Voting Equipment. . . . 11
2.5 Establishment Of The Election Center 12
2.6 New York Times Articles On Computerized Voting . . . 12
2.7 California Attorney General's Report 15
2.8 Texas Controversy, Hearings, And Legislation: 1986/1987. 16
    2.8.1 Controversy Over 1985 Dallas Mayoralty Contest 16
    2.8.2 Texas Secretary of State's Directive. 18
    2.8.3 Legislative Hearings. 18
    2.8.4 Revised Texas Statute on Electronic Voting Systems. 22

2.9 Current Problems Of Computerized Vote-Tallying . . . 23
    2.9.1 Difficulty in Verifying Results 23
    2.9.2 Possibility of Undiscoverable Frauds. 23
    2.9.3 Election Administrators' Lack of Knowledge and Resources 24

3. TYPES OF VOTE-TALLYING SYSTEMS, THEIR VULNERABILITIES, AND THEIR NATIONAL DISTRIBUTION. 25

3.1 Vote-Tallying As Part Of Voting. 25
3.2 Paper Ballots. 25
    3.2.1 Vulnerabilities of Paper Ballots. 26
3.3 Lever Machines 26
    3.3.1 Summarizing Lever Machine Results 27
    3.3.2 Vulnerabilities of Lever Machines 28
3.4 Punch Card Voting. 30
    3.4.1 Vulnerabilities of Punch Card Use 31
    3.4.2 Types of Punch Cards. 31
    3.4.3 Voting With the "Votomatic" Card. 32
    3.4.4 Vulnerabilities of the "Votomatic" System . . 33
    3.4.5 Voting With the "Datavote" Card 36
    3.4.6 Vulnerabilities of the "Datavote" System. . . 36
3.5 Voting With A Mark-Sense Ballot. 36
    3.5.1 Vulnerabilities of Mark-Sense Ballot Systems. 37
3.6 Precinct Versus Central Count For Machine-Readable Ballots. 38
    3.6.1 Vulnerabilities of Precinct Count and Central Count 38
3.7 Direct Recording Electronic (DRE) Machines 39
    3.7.1 Summarization of DRE Machine Results. 40
    3.7.2 Vulnerabilities of DRE Machines 40
3.8 Software For Computerized Vote-Tallying. 42
    3.8.1 Vulnerabilities of Software 43
    3.8.2 Integration of Administrative Software. . . . 46
3.9 Local Conduct Of Elections And Distribution Of System Types 47
    3.9.1 The Number of Major Election Jurisdictions. . 47
    3.9.2 Distribution of System Types. 48
3.10 Future Vote-Tallying Systems 49
    3.10.1 Technological Possibilities 49
    3.10.2 Political and Social Priorities 51

4. SOME RECENT DIFFICULTIES IN COMPUTERIZED VOTE-TALLYING . . 52

4.1 Carroll County, Maryland: November, 1984 52
4.2 Charleston, West Virginia: November, 1980. 55
4.3 Dallas, Texas: April, 1985 58
4.4 Elkhart County, Indiana: November, 1982, And November, 1986 64
    4.4.1 November, 1982 General Election 64
    4.4.2 November, 1986 General Election 68
4.5 Gwinnett County, Georgia: November, 1986 68

4.6 Illinois - Statewide Testing Program 70
  4.6.1 Programming and/or Program Initialization Errors. 70
  4.6.2 Hardware and Punch Card Difficulties. 72
4.7 Maricopa County, Arizona: September, 1986. 72
4.8 Moline, Illinois: 1985 Consolidated Municipal And Township Election. 72
4.9 Oklahoma County, Oklahoma: November, 1986. 74
4.10 Palm Beach County, Florida: November, 1984 78
4.11 Salt Lake County, Utah: November, 1980 79
4.12 Stark County, Ohio: May, 1986. 80
4.13 Summary Of Problem Types 82
  4.13.1 Insufficient Pre-election Testing 82
  4.13.2 Failure to Implement an Adequate Audit Trail. 83
  4.13.3 Failure to Provide for a Partial Manual Recount 84
  4.13.4 Inadequate Ballots or Ballot-Reader Operation 84
  4.13.5 Inadequate Security and Management Control. . 85
  4.13.6 Inadequate Contingency Planning 85
  4.13.7 Inadequate System Acceptance Procedures . . . 86

5. APPLYING INTERNAL CONTROL TO COMPUTERIZED ELECTIONS. . . . 87

5.1 Internal Control And Computer Security 87
5.2 Internal Control As Control Of Assets. 88
5.3 Voting And Banking Operations: Accounting Similarities 89
5.4 The GAO Concept Of Internal Control. 90
  5.4.1 Purposes of Internal Control. 91
  5.4.2 GAO Definition of Internal Control. 91
  5.4.3 GAO General Standards 92
  5.4.4 The Concept of a Non-Financial Transaction. . 94
  5.4.5 GAO Specific Standards. 94
5.5 A Classification Of Internal Controls. 96
  5.5.1 General Controls. 96
  5.5.2 Application Controls. 97
5.6 The Discipline Of Internal Control 98
  5.6.1 Link to a Professional Body of Knowledge. . . 98
  5.6.2 Job Functions for Internal Control. 99

6. DETAILED CONCLUSIONS AND RECOMMENDATIONS 101

6.1 The Continuing Problem Of Confidence In Results. . . 101
6.2 Responsibility And Requirements For The Effective Management Of Elections. 102
  6.2.1 Government Responsibility 102
  6.2.2 Expertise and Effective Management. 102
  6.2.3 Requirements. 104
  6.2.4 FEC Clearinghouse Performance Specifications. 104
6.3 Implementation Of An Internal Control Function . . . 104
  6.3.1 Outside Recommendations vs. In-house Expertise 105

viii

6.3.2 Achievement of Management Goals 105
6.3.3 Analysis of Risks and Impact on Public Confidence. 106
6.4 Review Of The Adequacy Of State Laws And Regulations 106
6.4.1 Revised Texas Statute on Electronic Voting Systems 106
6.4.2 Effective Use of Technical Terminology. . . . 107
6.5 Future Vote-Tallying Systems 107
6.6 Transfer Of Technical Knowledge To Election Officials. 107
6.7 Adoption Of FEC Clearinghouse Concepts For Product Acceptance 107
6.8 Software Certification, Performance, And Integrity . 108
6.8.1 Certification of Software 108
6.8.2 Requirements for Certification. 108
6.8.3 Integrity of Software 108
6.8.4 Dedicated Operation and Use 109
6.8.5 Logical Correctness of Vote-Tallying Software 109
6.8.6 Design for Specialization and Prevention of Logic Changes 110
6.8.7 Deposit and Availability of Certified Software. 110
6.9 Accuracy Of Ballot Reading 110
6.9.1 Accuracy Goal 111
6.9.2 Elimination of Pre-scored Punch Card Ballots. 111
6.9.3 Treatment of Rejected Ballots 111
6.9.4 Required Research 112
6.10 Design of DRE Machines 112
6.10.1 Recording of Each Undervote 112
6.10.2 Retention of Voter-Choice Sets. 113
6.10.3 Accuracy of DRE Machines. 114
6.11 Certification Of DRE Hardware Logic. 114
6.12 Selection Of A Vote-Tallying System. 114
6.13 Pre-Election Checkout. 114
6.14 Implementation Of Audit Trails 115
6.14.1 Full Ballots-Cast Data from Split Precincts . 115
6.15 Access Controls. 116
6.15.1 Site Controls 116
6.15.2 Equipment Access Controls 116
6.15.3 Transportation and Handling Controls. 116
6.15.4 Voting Process Controls 116
6.15.5 Telecommunications Security Controls. 117
6.16 Application Internal Controls For Ballot-Tallying Systems. 117
6.16.1 Controls over Blank Ballots Printed and Distributed 117
6.16.2 Numbering of Ballot Stubs 117
6.16.3 Controls over Ballot Use. 117
6.16.4 Control of Ballot Validity. 118
6.16.5 Machine-readability of Ballot's Precinct Number. 118
6.16.6 Accuracy of Telecommunication of Voting Data. 118

6.16.7 Control for Vote Summarization. 119
6.16.8 Vote Reconciliation by Contest. 119
6.16.9 Recording of Undervotes and Overvotes 119
6.16.10 Recounting. 119
6.17 Application Internal Controls For DRE Systems. . . . 121
6.17.1 Voter Count Match 121
6.17.2 Accuracy of Telecommunication of Voting Data. 121
6.17.3 Vote Reconciliations. 121
6.17.4 Recounting of Voter-Choice Sets 122
6.17.5 Post-Election Checkout. 122
6.18 The Recommendations In Relation To The Identified Problems 123

REFERENCES. 125

X

1. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

This report has been prepared with funding provided by the John and Mary R. Markle Foundation of New York City. The Markle Foundation requested that the National Bureau of Standards (NBS) undertake this study because of concern about the potential for inaccuracy or fraud in computerized vote-tallying. NBS was approached because of its experience with the subject matter as a result of a previous project undertaken by the author for the U.S. General Accounting Office.

Concern had been heightened by a series of articles published in the summer of 1985 in the New York Times. The articles cited statements by two computer experts reporting that a computer program widely used for vote-tallying was vulnerable to tampering. Several elections were identified in which losing candidates claimed that it would be possible to fraudulently alter the computer programs that were used in their contests.

1.1 Problems Of Computerized Vote-Tallying

In preparation for this report, a review of recent public statements and documents was undertaken that indicated concern about computerized vote-tallying. The review showed that the problems could be categorized as follows: there is difficulty in verifying results; there is the possibility of undiscoverable frauds; and election administrators lack some necessary knowledge and resources.

While proof of actual computer program manipulation appears to be lacking, documentation conclusively demonstrating otherwise is generally insufficient, due to the manner in which many computerized elections are conducted. It has been clearly shown that audit trails that document election results, as well as general practices to assure accuracy, integrity, and security, can be considerably improved.

1.2 Government Responsibilities

The recommendations that respond to these problems are directed to State and local government election officials. Elections for State and Federal offices are conducted by local government (generally county, township, and city) administrators. In about one-third of all counties, voting is carried out using computerized equipment. Jurisdictions using computerized equipment include over one-half of all registered voters.

Local administrators require the necessary resources and expertise to efficiently and effectively carry out their responsibilities. These responsibilities generally include procurement of vote-tallying systems and supporting services. An effective procurement must include specifications that assure accuracy, integrity, and security. The local administrators also have the responsibility for implementing the necessary management control systems to enable the public to have confidence in the results produced.

Election officials require a source of neutral expertise for the receipt of new technical and administrative information. The establishment of the Election Center in the Academy for State and Local Government clearly fulfills a need. Its efforts should be expanded.

1.3 Implementation Of An Internal Control Function

Internal control is a set of systematic procedures used to guard against errors, waste, and fraud. It is nearly universally used as a management technique to safeguard assets, and to protect operations that result in goods or services priced for sale. Voting services are not priced, and the discipline of internal control has not been systematically applied. Applicability of the discipline to vote-tallying requires only the re-definition of the concept of a transaction. A transaction is now defined as a business event that is measured in money and that is entered into accounting records; a re-definition would allow a transaction to include a step in the implementation of an entitlement that is not measured in money.

Essential recommendations are that the concept of internal control should be re-defined as indicated, and that persons knowledgeable in that professional field should be utilized to assist in the establishment and implementation of sound operational procedures. To the extent that procured computerized voting equipment and software must have capabilities that support internal control, applicable requirements should be included in procurement specifications.

Expertise in internal control (which includes computer security) should be added to the personnel complement in election administration in order to assure implementation of applicable concepts. In addition, an internal auditor should be available to independently review the implementation of internal controls and report on their effectiveness. Internal control is a professional activity; trained persons, texts, and a community of practitioners are available. Internal control expertise may be shared among government agencies or provided at the State level if individual agency resources are insufficient.

An important function of internal control is to identify system vulnerabilities and convert them into a set of realistic threats. Responses must be devised that are consistent with available or obtainable resources, based on a risk analysis determining the likelihood and cost of actual exploitation of a particular vulnerability. As a result, internal controls personnel should be able to provide assurances to the public that the potential threats are understood, have been prioritized for significance, and are being countered.

The availability of internal control specialists should relieve election administrators from having to be personally knowledgeable about specific technical matters best left to individuals who are professionally qualified in that field. With the addition of needed technical resources to the staff, election administrators would be able to retain management control. Administrators would not have to abdicate control to others, such as vendors or data processing center directors. Thus, election administrators would be able to retain the capability of managing the process of assuring accuracy, integrity, and security in vote-tallying.

1.4 FEC Clearinghouse Specifications

The performance specifications being developed by the National Clearinghouse on Election Administration of the Federal Election Commission (FEC Clearinghouse) are approaching completion. They are intended for Statewide adoption. Each State should consider the adoption of these specifications when they are issued.

Acceptance procedures for hardware and software should be consistent with the FEC Clearinghouse implementation plan for adoption of these specifications. That plan calls for qualification and certification prior to final acceptance. Qualification implies conformance with standards and functional requirements, and may be done once to satisfy many States. Certification ensures that the product meets State requirements. Acceptance testing evaluates the degree to which the specific units delivered to the local government conform to approved characteristics.

1.5 Revised Texas Statute On Electronic Voting Systems

The requirements of the revised Texas statute on electronic voting systems should be considered for adoption in those States that have not already adopted equivalent or more stringent provisions. Requirements of the Texas statute include audit trails, deposit of computer programs with the secretary of state, assurance that programs used in vote-tallying are identical to those deposited, mandatory one percent manual recount of all contests, testing of equipment using all applicable ballot formats, disconnect of remote terminals during vote tabulations, and specific scrutiny of ballot count discrepancies.

1.6 Recommendations On Software

1.6.1 Certification

Products to be certified should include all vote-tallying software and all software to be mounted together with vote-tallying software. Certification implies State approval. Only certified software should be permitted to be used within the State. After software has been certified, no design changes should be permitted without a re-certification. All software that has been certified should be deposited with the chief election official of the State. Consistent with the revised Texas statute, the materials on file should not be public information, but should be available to law enforcement authorities, on proper application, for investigation of election irregularities.

Specialization of vote-tallying software for a particular election should occur only with a "fill-in-the-blanks" procedure, not with logic design changes. Header cards used in vote-tallying operations should not change the logic of a program.

1.6.2 Integrity and Logical Correctness

As a requirement for certification, all vote-tallying software, and all software used with it, should be reviewed for integrity, that is, for the ability to carry out its asserted function and to contain no hidden code. Vote-tallying software should be tested, in addition, for logical correctness. Vote-tallying software includes software for election specialization and ballot generation, as well as vote-summarizing software. Satisfaction of the requirements may be done as part of qualification.

As part of the effort to maintain integrity of software, accountability of the source is essential. Copying of software from unaccountable sources must be forbidden. To minimize requirements for testing, all software should be obtained from a stock of products offered publicly by reputable vendors. Software that cannot be obtained in this manner must be thoroughly checked.

1.6.3 Dedicated Software Use and Dedicated Operation

An important procedure to assure system integrity is to isolate vote-tallying and support software from influences over which the election administration has no control.

After all software to be used together has been certified, it should be maintained separately under the control of the election administration and not used together with uncertified software. It is strongly recommended that certified vote-tallying software not be allowed to run on a multiprogrammed general-purpose computer on which uncertified support software or applications also are being run.

1.7 Recommendations On Hardware

1.7.1 Accuracy Of Ballot Reading

The value of a ballot-tallying system is that it should be possible, with a recount, to duplicate the result of an election. The problems found in ballot-reader inaccuracy, both in the count of ballots, and in the count of votes on ballots, are a significant source of lack of confidence in vote-tallying.

A recommended goal is that a computerized vote count should be able to be reproduced on a recount with no more than a change in one vote for each ballot position in ballot quantities of up to 100,000 when machine-generated (ideal) ballots are used. A ballot reader should be able to tolerate a wide range of punching or marking behavior by a voter without a significant increase in error.

1.7.2 Elimination of Pre-Scored Punch Card Ballots

The use of pre-scored punch cards contributes to the inaccuracy and to the lack of confidence. It is generally not possible to exactly duplicate a count obtained on pre-scored punch cards, given the inherent physical characteristics of these ballots and the variability in the ballot-punching performance of real voters.

It is recommended that the use of pre-scored punch card ballots be ended. One method now available to eliminate pre-scored cards, while retaining the "votomatic" concept, is with a new type of hole-punching stylus that uses spring-loading. A hole of consistent and acceptable dimensions can be created by a voter using the new stylus without the need for pre-scoring. The internal construction of the "votomatic" ballot holder must be altered with the use of the new stylus. Other devices and methods for elimination of pre-scored punch card ballots also may be effective.

1.7.3 Counting of Rejected Ballots

If a ballot cannot be read by machine, administrative controls should be in place to permit such ballots to be counted manually. A voter's choices should not be lost because of machine failure.

1.7.4 Required Research

Testing to determine the accuracy of current ballot reading systems (such as that now being carried out by ECRI of Plymouth Meeting, PA), and research to improve ballot tallying systems in accuracy and ease of voter use, are important to pursue.

1.7.5 Design of Direct Recording Electronic (DRE) Machines

With DRE machines, no ballot is used. The voter enters choices directly into a storage unit of the machine with the use of push-buttons, a touch-screen, or similar devices. As no voter-generated records of choices exist, and no recount independent of the machine is possible, steps should be taken in the design of these machines to assure complete confidence in the reported results.

A problem with most DRE machines as currently designed (as with lever machines, their predecessors), is that there is no difference in the results seen between a voter's failure to cast a vote and the machine's failure to record a vote.

Recording of Undervotes: It is recommended that each DRE machine be designed so as to take a positive action indicating a "no vote" for every choice that the voter fails to take. When voting is complete, the voter's choices, and any "no votes" for votes not taken, would be transferred to a more permanent storage for summation with other voters' choices. The required transfer and summation of the "no votes" would serve as positive indications of the voter's failure to make certain specific choices. Thus, there would be no ambiguity about whether the voter failed to vote or the machine failed to record selections.

Retention of Voter-Choice Sets for Summation Verification: Each voter-choice set (i.e., the machine's record of all choices of a voter) should be retained in the machine on a removable non-volatile medium (e.g., magnetic disk). Storage locations of the voter-choice sets would have to be randomized to prevent association of a particular set with a particular voter. The retention of the voter-choice sets makes possible a verification (on an independent machine) of the DRE machine's summation of the voters' choices that it recorded. The correctness of the machine's data entry process cannot be checked in this manner.

1.7.6 Certification of DRE Data Entry Logic

DRE data entry hardware should be certified for logical correctness, by examination of the logic design and by testing under a large variety of different conditions. The DRE data entry function must be correct, as there are no ballots to provide an independent check. The data entry logic and its documentation should be deposited with the State, as described above in 1.6.1.

1.8 Recommendations On Operational Procedures

1.8.1 Pre-Election Checkout

Lack of sufficient pre-election testing appears to be a major source of operational difficulty. Sufficient pre-election testing should be done so that errors in software specialization or in implementation of logical rules, if any, will become obvious. It is recommended that to the greatest extent possible, all hardware and software to be utilized should be given a dry run simulating specific conditions to be faced on election day and election night.

1.8.2 Audit Trails

Audit trails provide the supporting documentation through which the correctness of the reported results may be verified. Two types of audit trails are necessary to document operations and provide confidence in the results reported. One type records steps in the operation of the equipment, while the other records steps in the voting and vote-tallying processes.

1.8.3 Complete Data From Split Precincts

Each split of a split precinct should be treated like a separate precinct for the reporting of ballots and votes cast. However, voter privacy must be a concern for splits containing a very small number of voters.

1.8.4 Access Controls

Access (i.e., security) controls must be in place during preparations for voting, voting itself, and vote-tallying. These controls concern access to sites, areas, facilities, equipment, documents, files, and data. The controls cover transportation of ballots and telecommunication of results.

1.8.5 Application Internal Controls for Ballot-Tallying Systems

These controls should be in place to prevent all types of ballot frauds and miscounting errors, and to provide the documentation and assurance that the correct results are reported. Controls on ballots cover printing and distribution, accounting for use, validity, and prevention of errors due to mishandling. Controls on data and calculations provide for accurate telecommunication of data, recording of undervotes and overvotes, vote reconciliations that demonstrate consistency, and assurance of accurate vote summarization. A manual recount of at least one percent of the ballots of each contest is recommended. Responsibility for selection of some of the precincts to be recounted should be granted to candidates or parties.

1.8.6 Application Internal Controls for DRE Systems

These controls should be in place to provide documentation and assurance that the correct results are reported when DRE systems are used. The controls cover matching machine use with voter totals, vote reconciliations on each machine, recounting of voter-choice sets, and post-election checkout of machines.

1.9 Relative Vulnerabilities Of Different System Types

Each type of system has its own particular vulnerabilities. A comparison of system types shows that each has its advantages and disadvantages. It is possible to effectively utilize any of the computerized systems discussed (punch card, mark-sense, or DRE) provided that, among other requirements, procurement specifications are well-written in accordance with needed performance, and factors of accuracy, reliability, and recommended design concepts are included in the specifications.

1.10 Review Of Recent Difficulties In Computerized Vote-Tallying

Ten computerized voting situations in which difficulties occurred are reviewed in detail in this report. The four situations identified in the New York Times article of July 29, 1985 are among those reviewed. Problems in several other situations are briefly described.

Although none of the situations has provided solid evidence of computer program manipulation, the reviews have revealed the need for improvements in hardware and software performance and in operational procedures, and they have provided support for the need for institutional changes. Thus, the reviews have influenced the recommendations provided in this report.

Specific recommendations directly resulting from the reviews of difficulties include the recommendations on improved accuracy in ballot tabulation, elimination of pre-scored punch card ballots, assurance of the counting of ballots rejected by readers, provision of complete data from split precincts, and more thoroughness in pre-election checkout.

1.11 Future Vote-Tallying Systems

While vote-tallying using telephones or stations similar to automatic teller machines is technologically feasible, the decision to implement such a system must be based on more fundamental factors. Any installed system must meet political and economic requirements, as well as technical requirements of accuracy and reliability. Political needs include equal access by individuals, the ability to verify registration, and the ability of the voters to vote in secret without intimidation. Internal controls must be implementable to demonstrate the correctness of the reported results. Benefits, such as increased voter convenience and possible improved participation rates, must be compared against the costs of implementation.

2. BACKGROUND, AND RECENT SIGNIFICANT EVENTS

This report has been prepared in partial fulfillment of the conditions of funding received in November, 1986, by the Institute for Computer Sciences and Technology (ICST) of NBS from the John and Mary R. Markle Foundation of New York City. The Markle Foundation is privately endowed, and has a programmatic interest in the role of computer technology and communications in public affairs.

As a nonregulatory agency of the U.S. Department of Commerce, NBS was established in 1901 specifically to aid manufacturing, commerce, government, and academia through application of its expertise in science and technology. In connection with its consulting role, NBS may accept outside funding that is consistent with its mission and programs.

ICST carries out the responsibilities mandated to the Department of Commerce under the Brooks Act (P.L. 89-306). ICST develops techniques and tools to help organizations make more effective use of computers and information technology. In addition, ICST serves government and industry by developing Federal Information Processing Standards (FIPS), technical reports, and test methods, and by providing technical assistance to advance new uses of computer technology. In 1987, additional responsibilities were assigned to ICST due to the passage of the Computer Security Act (P.L. 100-235). In accordance with this act, ICST will develop standards and guidelines on computer security to protect the U.S. Government's sensitive but unclassified information.

2.1 Accuracy, Integrity, And Security

This report concerns measures to assure the presence of accuracy, integrity, and security in computerized vote-tallying. Accuracy is the essential requirement of a computerized vote-tallying system, but its achievement may not be possible without the implementation of integrity and security. Even if accuracy is attained, confidence in the results may not be assured unless the other two factors can be shown to be present. Thus, for vote-tallying systems, these factors are not mutually exclusive parameters that can be separately considered.

Definitions, for the purpose of this report, are as follows:

accuracy: conformity of the output data of a vote-tallying system with logically correct and acceptably precise treatment of all input data provided to the system;

integrity: the state of a vote-tallying system in which it will correctly perform the functions specified for it, and only those functions;

security: the achievement of a desired control of access to vote-tallying facilities, areas, equipment, supplies, documents, media, files, and data.

2.2 ICST's 1974/1975 Project On Computerized Voting

The origins of the current project go back to 1974. In February of that year, ICST was asked by the General Accounting Office (GAO) to "conduct a systems analysis and evaluation of the role of automatic digital processing equipment in the vote-tallying process." The year-long project, undertaken also by the author of this latest report, was completed in 1975.

The project had been requested by the GAO through one of its components, the National Clearinghouse on Election Administration of the Office of Federal Elections, in recognition of concerns expressed in Congress, and by election officials and the public, about the use of computing technology in vote-tallying. These concerns had been aroused by the issue of the potential for the fraudulent alteration of vote-tallying computer programs, and by actual difficulties experienced in computer-based elections. The possibility of fraudulent manipulation of computer programs had been raised by computer experts in Los Angeles in 1969. Serious problems in computerized vote-tallying had been experienced in San Francisco in 1968, in Los Angeles and Detroit in 1970, in Los Angeles and Houston in 1972, and in other places in the years immediately prior to the request for the report.

The product of the 1974/1975 project was a report entitled Effective Use of Computing Technology in Vote-Tallying [1]. The report identified the hardware, software, and administrative problems that had been encountered at that time, and specified operational guidelines that election administrators could implement to help assure the accuracy and security of the vote-tallying process. Several thousand copies of the report were distributed to election administrators throughout the nation by the National Clearinghouse on Election Administration. That organization, in 1975, had become a part of the newly established Federal Election Commission; it is identified elsewhere in this report as the FEC Clearinghouse.

2.3 Some Pertinent Technological Changes Since 1975

Since the 1975 report, there have been many additional experiences in the application of computerized vote-tallying, and considerable improvements in computer technology. In computer hardware, the most important changes have been improved speeds of operation, smaller physical size, and availability of larger quantities of random access and disk memory. The improved speeds and memory quantities are obtainable at considerable reductions in cost. The lower costs and improvements in technology have made possible the proliferation of smaller computers with considerable capability. Thus, it is now possible for many smaller election administrations to consider the acquisition of their own computing power, in order to achieve efficiencies and provide more direct management control over their operations.

There has been, also, continued improvements in tools and techniques for the management of technology. Tools include the availability of new standards in computer technology such as for media, programming languages, communications protocols, and data protection. Techniques include the concepts of software engineering, computer security, internal control, and EDP (electronic data processing) auditing.

The changes in computer technology, and the availability of new tools and techniques, have been considered in the development of the recommendations of this report.

2.4 Development Of Standards For Voting Equipment

In January, 1980, partly as a result of the 1975 ICST report, Congress adopted P.L. 96-187, Section 302, which stated that:

> "The Federal Election Commission, with the cooperation and assistance of the National Bureau of Standards, shall conduct a preliminary study with respect to the future development of voluntary engineering and procedural performance standards for voting systems used in the United States. The Commission shall report to the Congress the results of the study, and such report shall include recommendations, if any, for the implementation of a program of such standards (including estimates of the costs and time requirements of implementing such a program). The cost of the study shall be paid out of any funds otherwise available to defray the expenses of the Commission."

In 1983, the preliminary study was completed with the recommendation that "performance standards for voting systems are both needed and feasible." In 1984, the FEC Clearinghouse began to develop such standards. As of the summer of 1988, the hardware, software, and test standards for punch card, mark-sense, and DRE voting systems are approaching completion [2]. An executive summary of these standards also is being prepared [3]. The FEC Clearinghouse has also prepared a draft implementation plan for the voting system standards [4], and a "System Escrow Plan" [5]. The latter concerns the problem of controlling access to proprietary source code while States and local governments (or their agents) are provided with the ability to test the vote-tallying software for integrity.

Implementation of the standards would address some of the identified problems of computerized vote-tallying summarized below in section 2.9.

2.5 Establishment Of The Election Center

The Election Center, affiliated with the Academy for State and Local Government, was established in 1984. The Center is an independent non-profit resource center serving registration and election officials. National and regional election conferences sponsored by the Center, as well as reports and other data distributed to officials, provide training and information in some thirty-five areas of election administration.

The Center has recently distributed the report of a workshop [107] held on Captiva Island, Florida, in February, 1987. The workshop concerned computerized vote-tallying and included, as participants, election officials, vendors, computer scientists, and others interested in the election process. The workshop was funded by grants to the George Washington University by the John and Mary R. Markle Foundation. The Election Center had no part in the workshop but, because of its clientele, served as a convenient avenue of distribution for the report.

The Academy for State and Local Government is a non-profit research organization that fosters understanding of American government at all levels. The Academy is governed by a board of trustees composed of the executive directors of seven organizations representing States, counties, cities, and the chief officials of these jurisdictions.

2.6 New York Times Articles On Computerized Voting

A series of articles on computerized voting was published in the New York Times in 1985, commencing on July 29 of that year. In the first article, published on page one and entitled "Computerized Systems for Voting Seen as Vulnerable to Tampering" [6], it was charged that:

> "The computer program that was used to count more than one-third of the votes cast in the Presidential election last year is very vulnerable to manipulation and fraud, according to expert witnesses in court actions challenging local and Congressional elections in three states...
>
> "The vote counting program that has been challenged in Indiana, West Virginia and Maryland was developed by Computer Election Systems of Berkeley, Calif. In Indiana and West Virginia, the company has been accused of helping to rig elections. The computer program has also been challenged in Florida, but so far experts have not been permitted to examine the program in connection with the challenge.

> "John H. Kemp, president of Computer Election Systems, said in a telephone interview that he absolutely denied that the company was involved in fraudulent schemes. County officials involved in the cases also have categorically denied participation in fraud."

The article went on to state that allegations that the computer program provided by Computer Election Systems was "open to manipulation and fraud were supported by two ... experienced computer consultants who independently examined material obtained in the pending court cases for the New York Times." The two experts cited were Howard Jay Strauss, associate director of the Princeton University Computer Center, and Eric K. Clemons, an associate professor of decision sciences at the Wharton School of the University of Pennsylvania.

Mr. Strauss was reported as saying that "the program used to count Indiana votes was vulnerable to manipulation." He was additionally quoted as follows:

> " 'Extra votes may be entered in the form of bogus ballots on punch cards, or vote totals may be altered through the use of control cards,' Mr. Strauss said. 'Either of these assaults on the system could be performed successfully by a computer novice.'
>
> "Mr. Strauss added that someone with 'a fair amount of computer knowledge' could turn off the portion of the program designed to document any changes made in either the program or the votes being counted by the program."

However, an examination of the complete text submitted by Mr. Strauss to the New York Times shows that he also stated that:

> "If a better audit trail was part of the program, and if better procedures were followed in running the program, then all of the assaults on the system described above [for entering extra votes or altering votes] could easily be detected...

In addition, in response to the question, "Can the program be made safer?" Mr. Strauss responded:

> "...there is no way to design a tamper proof program. If prudent procedures are not followed in running it, any program can be compromised. The NBS publication Effective Use of Computing Technology in Vote-Tallying makes this point very clearly and provides reasonable guidelines for designing and running vote-tallying programs." [7]

These qualifying remarks were not reported in the New York Times article.

Professor Clemons was quoted in the July 29, 1985 article as saying that because of the excessive complexity of the program,

> " '...a doctored version of the code could be used to modify election results, and it would take weeks of study to determine what had happened.'
>
> " 'Code this complex is very difficult to trust,' Mr. Clemons said. One particular flaw that he cited was that 'the main program does not log all invalid ballots.' Another was that the printed log of error messages could easily by edited or altered."

An examination of the complete text submitted by Professor Clemons to the New York Times shows that he also stated that:

> "This does not mean that the code was constructed this way in deliberate violation of [FEC Clearinghouse] recommendations or current practice; this was a very common programming style in the 60s and mid-70s. And it does not mean that anyone is using the system to influence election results." [8]

These qualifying remarks, similarly, were not included in the New York Times article.

The July 29, 1985 article was distributed by the New York Times News Service, and also appeared, in whole or in part, in other papers, including the Greensboro (NC) News & Record and the Norfolk (VA) Virginian-Pilot.

Another article in the series, on August 21, 1985, entitled "Vote by Computer: Some See Problems" [9], reported that:

> "Many local election officials are baffled by computers and are unable to understand, question and challenge the computer systems.
>
> "Election system vendors are often forced by competitive bidding pressures to offer jurisdictions the cheapest possible systems, and the products they offer do not maximize fraud protection."

In explanation, the article continued:

> "The industry has been faced with competition to produce low-cost systems that can produce a quick tally, but it has not devoted much attention to devising systems that could be understood by local officials and

> that would provide features such as audit trails to make fraud difficult."

2.7 California Attorney General's Report

In December, 1985, the Office of the Attorney General of the State of California began a study that was "prompted ... by several nationally published news stories" [10], by which the New York Times series was meant. The study concentrated on "an analysis of the nature and extent of reported problems attending the computerization of the vote counting process" [11]. Almost every county in California uses computerized vote-tallying systems, and the systems include a significant number provided by the vendor named by the New York Times.

The report, on April 23, 1986 by Robert R. Granucci, Deputy Attorney General, might be summarized with the following quote:

> "My general conclusions are that while there have been no proven instances of vote counting fraud, certain concerns that have been expressed about the security and accuracy of computerized elections appear to have validity. However, these concerns are receiving serious attention and improvements are being made. A principal concern is that the most widely used vote counting software has been criticized for lacking a reliable audit trail and having a program structure that is very difficult even for computer professionals to understand.
>
> "It appears that most of the reported problems associated with computerized vote counting have occurred the first time the system is used by local election officials, and decrease in later elections. If experience is any guide, inaccuracies in tallying election results will tend to diminish as local election officials gain familiarity with electronic systems, but the potential for fraud may tend to increase.
>
> "The Attorney General should urge the Secretary of State to require that all electronic vote tallying systems have reliable, tamper-proof audit trails." [12]

(Note: compare final sentence above with Strauss quote in section 2.6 that "...there is no way to design a tamper-proof program. If prudent procedures are not followed in running it, any program can be compromised" [7]. It would seem that the essential need is for "prudent procedures.")

The Attorney General's report was publicized by the San Francisco Examiner in an article on October 20, 1986. The article reported that, according to the Secretary of State's office, which regulates elections, "in 25 years, no error has affected the outcome of a California election." However, there have been "sporadic glitches," the article reported. Several examples were given: in San Francisco in 1983, "an electrical power fluctuation during the vote count" added votes incorrectly to one candidate's totals; in Orange County in 1980, "a computer programmer's mistake" gave about 15,000 votes meant for two candidates to two other candidates; and in San Joaquin County in 1984, "a misplaced piece of punch card caused the system to indicate that one precinct had not been counted when it had been." [13]

The article also reported that:

> "'Rigging a computer vote would require a conspiracy of six to eight people,' said Deborah Seiler, head of the state secretary of state's computer voting division. 'The greatest possibility of error that I'm aware of is human error,' she said.
>
> "San Francisco Registrar [Jay] Patterson said that many election offices depend on manufacturers and county data processors to operate the systems. 'That certainly is not the best of situations when the person responsible for the vote count is not actually involved in it,' said Patterson.
>
> "Some counties with 'sloppy procedures' have failed to test computer equipment as required by the state, according to Robert Naegele, a technical consultant to the state and the Federal Election Commission. Each county must run 'logic and accuracy tests' of its system before and after the vote count." [13]

2.8 Texas Controversy, Hearings, and Legislation: 1986/1987

2.8.1 Controversy Over 1985 Dallas Mayoralty Contest

Following the April, 1985, Dallas mayoralty contest, Ms. Terry Elkins, campaign manager for losing candidate Max Goldblatt, approached the office of the attorney general of Texas with concerns about the manner in which the election was conducted. The attorney general's office asked a consultant to carry out an investigation. As a result of the investigation, Assistant Attorney General Robert L. Lemens wrote a letter to Ms. Karen Gladney, Director of Elections for Texas. The letter, on July 15, 1986, included the following statement:

> "...although [the consultant] has insufficient evidence to conclude that fraud has been committed, the electronic voting system in use lacks adequate security features to provide any assurances of the absence of fraud. As a result, this office has found that it will

> be difficult to demonstrate to the complainants that Texas elections are free from fraud and, thereby, free local election officials from suspicion." [14]

Further investigations followed by both the office of the attorney general and the office of the secretary of state (the latter included Ms. Gladney's office). On September 23, 1986, the Dallas Morning News reported the following story:

> "The state attorney general's and secretary of state's offices are investigating discrepancies found in the computerized voting records of several recent Dallas and state elections to determine if the results may have been obtained fraudulently...
>
> "The probe centers on allegations that computerized voting equipment and computer programs used to tabulate state and local elections may have been tampered with to bring about 'preprogrammed results,' [Attorney General Jim] Mattox said....
>
> "Terry Elkins, who managed [Max] Goldblatt's [1985] bid against [incumbent Mayor of Dallas Starke] Taylor, said ... that she has given to state officials 18 months of research documenting the discrepancies [in the 1985 mayor's race]. Chief among the discrepancies, she said is a claim that there were more votes cast than there were voters' signatures.
>
> "'The allegation is that the computer used to count the votes was given new instructions after it calculated that Max Goldblatt was leading Starke Taylor by 400 votes,' Mrs. Elkins said." [15]

(Note: A detailed discussion of vote-tallying problems in the Dallas 1985 mayoralty election is given in section 4.3.)

The following day, September 24, 1986, the Dallas Times Herald reported this additional information:

> "[Attorney General] Mattox said [on September 23] that the investigations call into question the ability of local city and county elections officials to vouch for the integrity of their elections when they use the automatic vote-tallying system.
>
> "The punch card system, which uses a computer to count ballots marked by voters, is so complex that election fraud could go unnoticed, Mattox said.
>
> "'I would say that the system appears not to have the kind of safeguards that election authorities would like

> to have to give them the independent capability to judge whether there has been fraud in an election,' he said.
>
> "'It would not be easy even for a computer expert to determine that there was fraud,' he said." [16]

2.8.2 Texas Secretary of State's Directive

As a result of the uncertainties created by the charges of vote fraud, and the ensuing investigations, the Secretary of State of Texas issued a directive on October 14, 1986 detailing additional security procedures for computerized vote-tallying to be used by county clerks and election administrators. The provisions of the directive were directly responsive to identified deficiencies in vote-counting procedures. Some of the provisions are as follows:

> "Under no circumstances may the computer-generated printed log of computer activity that occurs during the tabulation be turned off. The log must record all operator commands and inputs to the system from any device. The log must indicate for each precinct the total number of ballots that are entered into the central computer.
>
> "Each page of the log must reflect the correct time of day.
>
> "Each [of at least three cumulative reports produced throughout the tabulation process] shall include ...the number of over votes and under votes in each race.
>
> "... a computer-generated report that indicates the number of ballots cast in each precinct [shall be prepared].
>
> "... the secretary of state may order a manual count of ballots cast in the election to ensure the accuracy of the count." [17]

2.8.3 Legislative Hearings

On November 25, 1986, the Texas House of Representatives Committee on Elections, chaired by Representative Clint Hackney, held a hearing on possible changes in the election laws of Texas related to computerized vote tallying. Statements made by testifiers concerning the general problems of computerized voting included the following, by the indicated individuals:

Dr. Michael Ian Shamos, computer scientist, and one of three statutory examiners of electronic voting systems for the Pennsylvania Bureau of Elections:

"Punched-card systems have two significant positive features. One is that they cause a permanent physical record to be kept of every ballot cast....A second positive aspect is that cards can be counted very rapidly....

"...punched-card systems have no other redeeming features and in fact present great dangers. These are[:]

"...the ballot itself contains no candidate names and is meaningless when examined. This problem greatly increases voter confusion....

"The voter is unable to determine whether he has cast a complete ballot or whether he may have voted for more candidates that he is entitled. An overvote will result in an invalid ballot, and the voter's legitimate choices will go uncounted....

"It is a straightforward matter to alter a punched-card voting booth so that votes cast for one candidate will be recorded as though they were for another....Any required tampering can be performed during the election and all traces removed before any investigation can occur....

"....the computer hardware and software used to tabulate the ballots is subject to tampering. Furthermore, such tampering is relatively easy and invisible....Computers can be manipulated remotely, by wire or radio, or by direct physical input. The memories on which these computers operate can easily fit into a shirt pocket and can be substituted in seconds. The software can be set to await the receipt of a special card, whose presence will cause all the election counters to be altered. This card could be dropped into the ballot box by any confederate. The possibilities for this type of tampering are endless, and virtually no detection is possible once tabulation has been completed....

"Even if the software is not altered, there is no reason to believe that it is correct. Many tests performed on such programs have revealed faulty logic and wildly incorrect results.... Many jurisdictions, such as Pennsylvania, have complex rules for counting such situations as cross-filed candidates in vote-for-many offices and it is stretching to believe that an election system vendor would be aware of all such combinations of conditions to have produced perfect software. It is axiomatic in the computer industry that all large computer programs contain errors, and the more exten-

> sive the software the more errors it contains....
>
> "When one company or a conglomerate of companies supply unauditable software from a central distribution point, or participate directly in ballot setup procedures, there exists the possibility of large-scale tampering with elections. An errant programmer or tainted executive could influence or determine the outcome of a majority of election precincts in the country...." [18]

Ms. Suzan N. Kesim, vice-president of a security consulting firm of South Bend, Indiana:

> "The program for counting elections should use structured programming techniques. A detailed flow chart of the program should be required [to be submitted]....
>
> "Whether you are adding dollars or votes, you can apply many of the same auditing standards.... Many of the computer auditing procedures used by the banking industry that have been tried and true could easily be modified or used as they are for auditing elections....
>
> "Pre-punching the ballots with the precinct could be a really crucial way of checking and making sure that ballots don't slide from precinct to precinct....
>
> "Fraud possibilities include 'hidden programs'....
>
> "Write a public domain software program to count votes, open to public scrutiny...." [19]

Anita Rodeheaver, County Clerk, Harris County (Houston), Texas:

> "A computer, whether it is in a bank or a hospital or a collection agency, or being used for elections, is only as good as the people that run it....
>
> "It upsets me when continually we work so hard to have good honest elections and we continually get hit with things that could happen or 'supposedly are happening,' but no one ever comes up with any concrete evidence that they did happen...." [20]

Tom Eschberger, Vice-President of Business Records Corp.:

> "In twenty years, I have seen two cases of attempted fraud on an election system. I saw one in Albuquerque, New Mexico on lever machines, and one in Pueblo, Colorado attempted on punch cards. I have personally run about one thousand elections around the country.... Those were the only two cases where I was convinced

> that somebody had tried to defraud somebody.
>
> "I have seen a lot of cases where people make dumb mistakes, where the totals don't add up.... Elections are run by amateurs. [Other than experienced election administrators,] there are 400 people out in the precincts who got just a one-hour training class. People are not going to have perfect elections. People are going to have the best elections that well-intentioned honest people can run, and that well-intentioned honest companies can run....
>
> "A lot of counties want us to do the programming for them because it disassociates them from any candidate and any accusation of fraud or collusion.... [Persons intending to commit fraud would] have to have our source code, they would would have to have collusion with somebody in the county, they would have to have access to the computer....
>
> "[Filing the program with the secretary of state] might set some minds at ease. Then, someone could look at the code and know what's going on in an election if there were a problem. If someone said there was fraud and here's how they did it, then you have someone at the State level who is familiar with our source code that could say yes or no. Yes, it would be beneficial from that standpoint." [21]

Warner Croft, a partner in the public accounting firm of Arthur Anderson and Company:

> "We do believe the election laws need to be codified to reflect the technology being employed today in the election process.
>
> "We do believe that the Secretary of State needs to have the authority and the money to enforce those laws, to make sure that the proper audit trails are in place, so that whenever allegations do surface, ... the records are in place so that the State can, with a minimum of time and effort, go to those records and find out what happened.
>
> "Unfortunately, the laws at this time are a bit too nebulous for that to be done....
>
> "As long as there are winners and losers in elections, regardless of the system being used, there will be these allegations. You cannot legislate this problem away by requiring a higher generation of technology, another language.

> "But what we can do is require an audit trail, so that the documents that represent the voter's intent are kept on file, for a predefined minimum period of time, so that no matter what went on inside the computer, we've got a source that we can go back to, to determine what the voter actually did...." [22]

2.8.4 Revised Texas Statute on Electronic Voting Systems

A revised statute on the use of electronic voting systems was passed by the Texas legislature and was approved in June, 1987 [23]. It took effect on September 1 of that year. Some of the revisions concerned the following topics:

Auditing: A voting system may not be used unless it is capable of providing records from which the operation of the system may be audited.

Deposit and Comparison of the Program: Copies of the "program codes" and related documentation must be filed with the secretary of state. The secretary of state must periodically compare the materials on file with those materials actually used to ensure that only approved materials are used. The software on file is not public information, although it may be made available to the attorney general for investigation of irregularities.

Use of Remote Terminals: Computer terminals located outside the central counting station must be capable of "inquiry functions only" during vote tabulation, and "no modem access to the tabulation equipment" must be available during tabulation.

Testing of Equipment: Each unit of tabulating equipment shall be tested "using all applicable ballot formats."

Discrepancies in Ballot Totals: If, in the use of a precinct-located computer, a discrepancy of more than three exists between the number of ballots recorded by the computer and the number of ballots written down by the precinct officials, the final count of that precinct shall be done centrally.

Manual Count: A manual count of all the races in one percent of the election precincts, but in no less than three precincts, shall be conducted at the local level. The secretary of state also may conduct a manual or automatic count of any number of ballots. No specific ground for obtaining an initial recount is required.

As a result of passage of the revised statute, all electronic voting systems now certified for use in Texas will need to be re-certified. The revised statute specifically addresses some of the problems of computerized vote-tallying identified immediately below.

2.9 Current Problems Of Computerized Vote-Tallying

Current problems of computerized vote-tallying, including those identified by those who have recently made public statements or produced public documents, are summarized by the following categorizations. The relationship of the recommendations of this report to these problems is discussed in section 6.18.

2.9.1 Difficulty in Verifying Results

Results of elections announced by election officials are difficult to verify. The problem of verifying results is due to:

(a) lack of audit trails;
(b) poor design of computer programs;
(c) vendor-supplied computer programs that are unavailable to the scrutiny of responsible officials;
(d) administrative procedures that are incomplete and poorly implemented, resulting, for example, in the inability of observers to successfully compare computer reports of ballots cast with the same data reported by precinct officials.

2.9.2 Possibility of Undiscoverable Frauds

The lack of internal controls and failure to implement computer security increase the possibilities that unknown persons may perpetrate undiscoverable frauds. Methods of forcing incorrect results include:

(a) fraudulent alterations in the computer program or in control cards that manipulate the program;
(b) activation of a hidden program, possibly by means of a time-of-day match or with a specially encoded punch card ballot;
(c) manual replacement of the computer program by a fraudulent substitute;
(d) introduction of false ballots into the set of real ballots, through either addition or replacement; or introduction of false ballot data through interchange of ballots, by a perpetrator taking advantage of different ballot styles;
(e) introduction of false voting summaries through changes in data stored in removable data storage units of precinct-located, vote-counting devices;
(f) fraudulent alteration of the face of the voting device used by the voter at the polling location to mark a ballot or indicate choices;
(g) fraudulent alteration of the logic of precinct-located, vote-counting devices.

2.9.3 Election Administrators' Lack of Knowledge and Resources

Some election administrators have a lack of knowledge about computers, and they lack the necessary knowledge and resources to effectively negotiate with vendors. The effect of these deficiencies are:

(a) administrative errors in conducting elections, with increased potential for fraud or, at minimum, loss of public confidence;

(b) abdication of control over elections to vendors and county data processors, with the resultant inability to impose the necessary internal controls;

(c) inability to require vendors to provide computer programs, election equipment and supplies that include adequate safeguards against fraud and inaccurate reporting;

(d) increased risk to vendors in entering a market fraught with the potential for negative publicity, resulting in reduced competition and reduced investment in improved products;

(e) slower than adequate introduction of more effective technology.

3. TYPES OF VOTE-TALLYING SYSTEMS, THEIR VULNERABILITIES, AND THEIR NATIONAL DISTRIBUTION

3.1 Vote-Tallying As Part Of Voting

Voting, as it is carried out in the United States today, may be said to consist of four distinct administrative steps. These are:

(1) voter authorization: the determination of whether the prospective voter is entitled to vote at a particular place, and for what set of offices and issues;

(2) secret choice: provision of the opportunity for the voter to express his or her choices without intimidation:

(3) precise recording of the expression of each voter's choices in a voter-disconnected and easily countable format; and

(4) accurate summarization of all voters' choices by candidate and issue alternative.

Vote-tallying, a subset of voting, consists of steps (3) and (4), although the process involves concern for steps (1) and (2).

3.2 Paper Ballots

The uniform use of an official ballot containing the names of all candidates, printed on uniform paper by public officers at public expense, and distributed only at the polls where it is marked in secret, was adopted first in the Australian state of Victoria in 1856. In the years immediately following, the concept was adopted in other Australian states. Thus, it came to be called the "Australian ballot" [24]. The Australian ballot concept was the first successful attempt to meet the requirements of steps (2) and (3) above.

The Australian ballot had its first U.S. statewide application in New York in 1889, and was adopted widely throughout the Nation in the next decades. Prior to that, the application of the secret ballot was limited. In many cases, persons had to announce their votes publicly, or tell them to a sheriff who recorded them. In other cases, there were party-specific paper ballots, produced with different colors or weights of paper to reveal party choice.

During the early years of introduction of the Australian ballot, there was considerable controversy over whether the information on the ballots should be arranged in a "party" format (the set of all candidates of a single party listed together), or in an "office" format (the set of all candidates for a single office listed together). At present, most ballots are designed with an "office" format. However, in many states, voters are permitted to select all candidates of a particular party with a single "straight party" vote, with an allowance for "crossover" votes for specific candidates of any other party.

Paper ballots remain in use today in small communities and rural areas by about eleven percent of U.S. registered voters (see section 3.9.2 for the percentage of use of the various system types by counties and by registered voters).

3.2.1 Vulnerabilities of Paper Ballots

When effective administrative controls are not applied, paper ballots are subject to possible fraud and error in their distribution, in their use at polling places, and in counting.

Ballot frauds: Failure to properly account for ballots distributed may provide the opportunity for fraudulent addition of extra ballots into the ballot box, an activity generally referred to as "ballot stuffing." In places where votes are bought and real ballots are not sufficiently distinctive, voters may be handed pre-voted counterfeit ballots before entering the polling place. As an alternative fraud, voted counterfeit ballots may be substituted for real ballots already voted.

Chain voting: When administrative controls at the polling location are poorly implemented, and enough voters are willing, chain voting is a possibility. In chain voting, the first voter in the chain retains the unvoted ballot given to him at the polling place and, instead of voting, takes the ballot outside. This voter loses his vote, but starts the chain. Outside, a party worker fills out the ballot and hands it to a second voter who has also agreed to participate. The second voter turns in the voted ballot, but retains the unvoted ballot handed to him in the polling place for return to the party worker outside. Successive voters who participate receive a pre-voted ballot and return an unvoted ballot to the party worker.

Malicious invalidation: In counting paper ballots, extra marks may be made on ballots intended for an opposition candidate, thereby subjecting those ballots to invalidation in jurisdictions where extra marks are cause for that result. (Extra marks are often cause for invalidation because such marks may be used to indicate that a private agreement has been carried out in which a voter has agreed to vote as instructed in return for some consideration.)

Inaccurate counting: Hand counting of large numbers of paper ballots is generally inaccurate, because of human inattention and fatigue, compared with counting of machine-readable ballots.

3.3 Lever Machines

The first use of mechanical lever-type voting machines was in Lockport, New York in 1892 [25]. In the use of these types of machines, hereinafter referred to as "lever machines," each candidate or issue alternative is assigned a particular lever of a rectangular array of levers on the face of the machine that is seen by the voter. The levers are horizontal in their unvoted positions. The array of levers may be arranged with offices from right-to-left and parties from top-to-bottom, or vice-versa. A set of inserted printed strips visible to the voter identifies the lever assignments.

On entering the area of the machine (the "voting booth"), the voter enables the machine with a handle that also closes a privacy curtain. Then, in order to indicate choices, the voter pulls down selected levers. When the voter exits the voting booth by opening the privacy curtain with the handle, the levers are automatically returned to their original positions. As each lever returns, it causes a connected counter wheel within the machine to turn one-tenth of a full rotation. The counter wheel, serving as the "units" position of the numerical vote count for the associated lever, drives a "tens" counter one-tenth of a rotation for each of its full rotations. The "tens" counter similarly drives a "hundreds" counter. If all the mechanical connections are fully operational during the voting period, and the counters are initially set to zero, the position of each counter at the end of the voting period indicates the number of votes that were cast on the lever that drives it.

By 1930, lever machines had been installed in Denver, Milwaukee, Minneapolis, Newark, New York City, Pittsburgh, Philadelphia, and San Francisco [26]. One reason for the acceptance of the machines was the existence of significant fraud in the use of paper ballots. By the middle 1960s, just before the introduction of punch card voting, almost all large cities and many medium-sized ones used lever machines. It is likely that, at that time, over one-half the votes in the Nation were being cast on lever machines (now slightly more than one-third).

Lever machines are precinct-located devices, that is, the basic vote-count is accomplished at a neighborhood voting location that may be remote from the place where the votes are summarized to determine the outcomes of the contests. The number of machines at each location depends on the number of persons expected to vote there and the expected average time for a person to cast a complete set of votes. Separate machines may be required for each party in a primary election (conceivably, only part of the machine could be made operable for a voter of a specific party, with another part reserved for another party) and for each precinct voting at the same location.

3.3.1 Summarizing Lever Machine Results

After the close of the polls, the backs of the machines are opened. The number of votes is read off each of the counters, and each number is transcribed to official documents. Recently manufactured lever machines may allow for printing of the counter values on request. The official precinct documents are carried to the central vote-counting location for summarization.

With lever machines, only summarized voting results are available at the precinct level. No individual choices are available to be counted. Interlocks in the machines prevent overvoting (voting for more than the allowed number of candidates in a contest, e.g., voting for three candidates in a vote-for-two contest, such as for school board). There can be undervotes (voting for less than the allowed number of candidates in a contest, e.g., voting for one or no candidate in a vote-for-two situation).

3.3.2 Vulnerabilities of Lever Machines

With a lever machine, there is no ballot, i.e., no independent verification of each machine's recorded result. While the lack of ballots eliminates the possibility of chain voting, counterfeit ballots, and spoiling of the opponent's ballots, there are other possibilities for fraud or error, some available because there are no ballots.

Vote count frauds: The lever-machine equivalent to "ballot stuffing" is the casting of extra votes on the machine by party workers. When there is no genuine bipartisan staffing of a precinct polling place, any type of vote-tallying system is more easily subjected to fraud.

No audit trail of voter's intent: One effect of the unavailability of ballots is the lack of a true audit trail. No unequivocal distinction between an undervote and a machine failure can be made solely with a review of the vote counts. If the number of votes cast for an office is less than the number of persons that have voted on the machine (often indicated by a "public counter" that may be connected to the voting handle), then for each undervote, there are the following possibilities for a contest involving two candidates: either the voter failed to vote for either candidate, or the counter mechanism failed to turn for the voter's choice.

In general, it is not possible to determine which one of these possibilities is the correct one for any single undervote without a review of the internal condition of the machine. If a counter mechanism failed to turn, it may be due to an actual disconnect in the mechanical system, or it may be due to excessive friction in the connections. If a vote total reads 000 or some number up to 009 when many more might have been expected, a mechanical disconnect is a strong possibility. If a vote total reads 009 or 099, the possibility is increased that excessive friction at the point of highest mechanical resistance to turning (during an arithmetic carry operation) caused a failure. If the counter failed to turn correctly for any reason, there is no independent ballot available to verify the count. The voter's choices are lost, absent a court order for a new election.

No true recount capability: In a lever machine contest, a "recount" simply means that the precinct transcriptions are reviewed to determine if any precinct official erred in copying down the counter values or the precinct documents were fraudulently replaced on the way to the central summarization location.

Write-in difficulty: Another problem with lever machines is the difficulty of indicating write-in votes. The lever machine is not oriented towards individual idiosyncratic choice, but only choice from the available menu. If State or local law requires it, a roll of paper is made available with the machine for use by a voter in writing a name not available on a lever. However, the selection and use of this mechanism is noisy, and it is obvious to those around the voting area that a write-in vote is in progress. Since only a small number of voters may choose this possibility, privacy may be completely lost by those individuals in that instance.

Mis-labeling: A possibility for error or deliberate fraud is the insertion of incorrect identifying strips on the front of the machine, so that the levers are mis-identified to the voters.

Storage and transport: Lever machines are large and heavy, and therefore difficult to transport and expensive to store (compared with precinct-located electronic machines).

Setup errors or frauds: "Programming," i.e., pre-election setup with interlocks, requires specialized knowledge and is labor-intensive. Furthermore, the necessary specialized knowledge is not directly translatable to a variety of other work, for the support of the machine technicians between elections. As with any other situation where specialized knowledge may be employed for honest or dishonest purposes, the possibility of collusion involving lever-machine "programmers" must be considered.

Difficulty in operability verification: It is difficult to statistically test the correct operation of a lever machine by applying a large number of test votes. A lever machine is operated by direct human action, and the use of human labor to insert a statistically significant number of test votes to each counter would be expensive and error-prone. To effectively accomplish a statistical test of correct operation, a mechanism would need to be constructed that could vote on each lever a large number of times with an electromechanical drive that could be programmed. The mechanism would check the following: the single-vote recording operation of each counter, proper implementation of vote-for-more-than-one setups, overvote prevention, and proper operation of the arithmetic carry mechanism.

3.4 Punch Card Voting

Voting systems based on punch card ballots began to be used in the middle 1960s, and received considerable application in the western part of the U.S. by 1972. At that time, about 10% of U.S. voters used punch card ballots to record their choices [27] (but now, almost 45% use one of the two principal types of cards).

The introduction of punch card voting was an economic choice of many communities in their efforts to provide election services to an expanding population. Voting with punch cards does not require serial processing of many voters through a single voting station containing a complex machine. Several voting stations may be made available in one precinct with much less expense.

In the late 1960s and 1970s, punch card input of data to mainframe computers was commonplace. Punch card stock and punch card reader technology were widely available. American national standards, developed to specify the size of the cards [28] and the arrangement of holes in each card [29], were available to be adopted for punch cards used in voting.

The standard punch card has 960 potential punch locations arranged in 80 columns by 12 rows. In common business use, each column on a card represents one character (such as a letter of the alphabet or decimal digit). A standard data code for business use of the punch card has been developed, and it is called the Hollerith code [30]. In this code and in its recent extensions, a graphic character (a character seen in printed text) typically requires no more than three holes in a column to represent it. For each unique character, the holes representing it form a correspondingly unique pattern. When the pattern of holes in the twelve locations in one column is read by a card reader and converted to a sequence of 1s and 0s in a computer (e.g., 1 for a hole and 0 for no hole), the sequence may be recognized as the unique character by a computer program.

When the standard punch card is to be used to record votes, it is necessary to permit more variability in the use of punch locations than the Hollerith coding system allows. When any number and arrangement of holes in a single column are permitted, the coding system is called "column binary." However, not every location on the card can be used for voting. This restriction is generally due to ballot layout considerations, but some consideration must be given to the physical strength of the card when it is used with more intensive layouts. A further limitation on the use of punch locations is necessary if information about the candidates and issue choices is to be printed on the card.

3.4.1 Vulnerabilities of Punch Card Use

Punch card ballots have all of the vulnerabilities of paper ballots that are related to distribution, precinct use, and collection. Administrative controls may be implemented to prevent the typical paper ballot frauds. Most of these controls have been previously identified [1], and are proposed again in section 6.16.

Manufacturing requirements: Accurate dimensioning in manufacturing, and use of materials consistent with the needs of punch card readers, are additional requirements unnecessary for paper ballots.

Ballot-reader requirements: Accurate ballot reading is of fundamental importance in a punch card system. Assurance should be obtained, in both pre-election and post-election checkout, that the readers are correctly reading the ballots. In addition to the question of accurate recording of voters' selections, difficulties in ballot processing may include card jams, transport of more than one ballot at a time, and the inherent problem of pre-scored cards. If a card jams in the reader, it is essential to know whether or not the card was counted; otherwise, either the card and its votes may be counted twice, or not at all. Transport of more than one ballot, similarly, may cause a miscount of the cards as well as inaccurate reading. (The reader can accurately read only one ballot at a time.) The problem of pre-scored cards is considered in sections 3.4.3 and 3.4.4.

3.4.2 Types of Punch Cards

Two common types of punch cards used for voting may be distinguished. These are designated in popular usage as the "votomatic" card type and the "datavote" card type. As used by a voter, a card of either type is positioned with the long edges on the right and left, and the short edges at the top and bottom. Thus, each column is horizontal, and each row is vertical. The card is usually issued to the voter with a numbered stub attached to the top short edge. The line of attachment is perforated for easy removal of the stub. In most cases, the stub is removed immediately before the ballot is submitted; it may be removed by a precinct official while the voter's choices are covered by an envelope or other holder. One use of the number on the stub is to assure that the ballot voted is the same one issued to the voter.

"Votomatic" card: With the "votomatic" card, the locations at which holes may be made to indicate votes are assigned numbers. The number of each hole is the only information printed on the card. This type of card maximizes the number of voting locations available. As there is no space on the card for names, names of write-in candidates must be written by the voter on the envelope provided to the voter with the card. In the tallying process, each envelope must be examined before the card is removed; each card and its envelope with write-ins must be put aside for separate processing. The envelopes with write-ins cannot be separated from their ballot cards until the cards are reviewed for overvotes.

In the 312-position "votomatic" card, every third column is used, beginning with column 5 and ending with column 80. This allows for 26 usable columns which, when combined with 12 rows per column, provides for 312 positions. There are also 228-position and 235-position cards available. Only one side of the "votomatic" card is used. The "votomatic" card (when separated from any attached stub) is generic for any election, as it only has numbers on it.

"Datavote" card: With the "datavote" card, the name of the candidate or description of the issue choice is printed on the card next to the location at which the hole is to be punched to indicate the choice. Fewer voting locations are available on the "datavote" card. However, the "datavote" card provides a particularly simple write-in capability, as a separate blank candidate line in each contest may be provided for that purpose.

For the "datavote" type card, the locations used for voting are in a row close to the righthand long edge of the card. Spacing of two or more columns between voting locations is required to allow room for the printing of the candidate name or issue choice description. Typically, the card may be turned over (with its long dimension as an axis) so that the other long edge is on the right. Then, the other side of the card and a row close to the second long edge may also be used to provide voting locations.

3.4.3 Voting With the "Votomatic" Card

A voter uses the "votomatic" card for voting by first inserting it (with its attached end stub) in a hollow mechanical holder. (The holder is often called a "votomatic device" or "vote recorder.") The stub contains two holes. The card is properly positioned when the holes in the stub are fitted over two small posts on the device. The holes are assymmetrical in the stub to prevent the voter from inserting the card so as to show its reverse side. The system was developed from a concept introduced by Dr. Joseph P. Harris, whose early book on election administration has been previously referenced [24], [25], [26].

Compared with the lever machine, the mechanical holder is inexpensive. Many more holders could be used in a precinct for the same cost, and therefore, more voters may simultaneously vote.

A hinged booklet is attached to the mechanical holder. The booklet is attached so that it is centered over the inserted punch card. The pages of the booklet are crimped to a hinge, as it is necessary that the pages not be removed during the voting process. The attachment permits the exposure of only one row of the punch card to the view of the voter at the axis of the booklet. As the pages are turned, a different row of the punch card is exposed for each page. All voting instructions, such as office names, candidate names, candidate punch positions, and allowable number of votes per office, are presented on the pages. (In some cases, the pages are simply transparent envelopes and the ballot information is provided on inserts within the envelopes. In those cases, the envelopes are sealed following insertion of the ballot information.) The names of the candidates and issue choices must be positioned on the pages so that each is next to the appropriate voting location on the card.

A vote is cast by creation of a hole in the punch card at the desired location. Almost all unvoted "votomatic" cards are prescored, i.e., each voting location on the unvoted card is scored in the shape of a rectangle. Sufficient pressure on the voting location with a hand-held stylus forces out the inside of the rectangle, identified as a piece of "chad." The need for prescoring is due to the simple nature of the stylus and the inability of the voter to otherwise form a hole of the dimensions required for processing through a ballot reader.

Recently, a new type of stylus has been introduced: one which does not require a pre-scored card. The new stylus has a spring-loaded sleeve. The sleeve provides sufficient force to punch out pieces of round chad with a diameter acceptable for processing, without the need for pre-scoring. The new stylus is used with the same type of "votomatic" ballot holding device as that used for pre-scored cards, but with a change in the device's internal construction. Precise manufacturing of the new internal "templates" that guide the stylus is required. This type of system has been used successfully in St. Lucie County, Florida. St. Lucie has about 400 ballot holder units constructed for use with the new stylus.

3.4.4 Vulnerabilities of the "Votomatic" System

Some vulnerabilities that are special to the "votomatic" system include the following: the lack of candidate information on the card itself, the need of the voter to turn over all the pages of the booklet to get all available voting information, possible misalignment of the candidate information on the page with the appropriate voting location on the card, the possibility of malicious alteration in the voting instructions on the pages, and the problem of chad in pre-scored cards.

Lack of candidate information on the card: The fact that the "votomatic" card only has numbers on it results in a lack of an obvious relationship to the candidate selected, once the voted card is removed from the mechanical holding device. However, each hole is numbered, and the instructions on the pages identify each candidate and issue choice by the corresponding hole number. In jurisdictions that use the system, campaign advertising may specify the hole number of the desired choice (although rotation of candidate sequence in different districts prevents candidates running in multiple districts from having a universal card location).

In absentee voting, the voter typically does not have a ballot holder available. The voter must find the number of the candidate or issue choice desired as listed on the instructions, find the number on the ballot that matches the number of the candidate, and punch out the corresponding chad.

Clearly, the system is not as user-friendly as a ballot or display containing the candidate names, on which each vote is cast next to the desired name, but the "votomatic" system may have been selected because of economy, or the presence of a very long list of contests, for which no viable alternative voting system exists. In California, each voter receives a sample ballot in the mail. Knowledgeable persons in that state believe that this procedure significantly improves the voter's ability to correctly use the system.

Need to turn over all pages: The voter must turn over all the pages of the booklet to obtain all necessary instructions and to permit each voting location to be available for punching. Some voters may forget to do this and lose their franchise for some contests and issues. When the number of candidates for a single office is very large, the voter may be forced to look on successive pages to find the total list. Confusion about voting for such a contest may result. If the "votomatic" system is selected for other compelling reasons, voter education is the only method of assuring voter understanding of the voting process.

Failure of information alignment: If assembly of the mechanical holder and the booklet is inaccurate, or the location of printing on the pages is imprecise, the candidate information on the pages may not correspond exactly to the appropriate voting location. Voter confusion, about which hole to punch, will result.

Malicious alteration of instructions: It has been charged (see section 2.8.3) that the instructions on the pages might be altered by a particular voter, to the detriment of voters who follow and use the same mechanical holder. Even if the holder could not be easily taken apart by a voter and the pages replaced, certainly the instructions could be defaced or covered over with a stick-on label that supplies false instructions. A defense against this is alertness on the part of the precinct officials, but there are other defenses in place. One defense is that the perpetrator will have given his verified name and address. Secondly, the perpetrator may be observed if there is no privacy curtain; or a following voter may note the defacement or alteration, thus limiting the possible perpetrators to a small number. In addition, since many mechanical holder units are employed in a typical election, the damage done will have a very small effect, unless a massive conspiracy attacking many such units can be assembled.

Problem of chad in pre-scored cards: Pre-scored cards have presented some difficulties in processing. Either a chad may fall out unintentionally, or a chad that is intended for removal may not be fully removed. In either case, the voter's intent is not accurately recorded.

A chad that is not intended to fall out may be loosened in handling, or may be loosened in the processing of the card through the card reader. Lack of care in tearing off the stub of the card may loosen chad. Undesired removal of chad in reading may be more likely if the design of the reader mechanism requires the card to bend. If the card jams in the reader and is folded or bent, pieces of chad may fall out. Training of precinct personnel in card handling and stub removal, and careful selection of card readers, may alleviate this problem.

During voting, a piece of chad completely removed by the voter should fall into the mechanical ballot holder and cause no difficulty. However, in some cases, the voter fails to completely remove the chad. This problem may be due to one or more of several factors, such as: (a) the mechanical holder may have been constructed or assembled poorly, and the parts of the holder are not where they should be, (b) the materials are of poor quality, or certain materials used, e.g., rubber, may have deteriorated with time, (c) the voter may have inserted the punch card incorrectly into the mechanical holder, (d) the voter may attempt to punch out the chad with a less effective tool than the stylus, such as a ball point pen, (e) the voter may apply insufficient force, because of a physical infirmity or because the voter is unaware of the requirement for complete chad removal, (f) the dimensions of the punch card may not be within tolerances, or (g) the process of pre-scoring the card might have been done poorly.

A partially removed chad may be pressed back into the card during the stacking of the cards in preparation for reading, or during the reading itself. If the chad is pressed back, no vote will be recorded for that location, even if it was the intention of the voter to cast that vote. A chad that falls out during the reading process may affect the operation of the reader. Some election administrations provide "inspection boards:" bipartisan panels of persons who review each card before processing, and who remove hanging chad according to pre-established rules. This process also identifies write-ins, and catches the occasional malicious action, such as the attachment of chewing gum or other objects to a card. Extraneous objects may cause the card to stick in the card reader, or possibly damage the reader mechanism.

3.4.5 Voting With the "Datavote" Card

For voting on the "datavote" card, a stapler-like tool is used. The tool creates a hole instead of inserting a staple, and the tool provides sufficient force such that pre-scoring of the card is unnecessary. In order for the tool to be used, the card is placed in a holder which positions the row to be punched under the hole-punching part of the tool. The tool is mounted on the holder so that it can move up and down the row to the desired column. The holder is inexpensive, so that several may be used at one voting location.

3.4.6 Vulnerabilities of the "Datavote" System

With the use of the hole-punching tool, there is no problem of hanging chad. Since the candidate information is on the card, there is no potential for malicious alteration of voting instructions.

Multiple cards: As the "datavote" card provides fewer voting locations than the "votomatic" card, even when both sides of the "datavote" card are used, more than one "datavote" card may need to be issued to a voter. Additional cards require a certain additional expense. In using the "datavote" system, a voter may forget to turn the card over, or forget to use the additional cards, thereby losing part of the franchise. As with the problem of turning over the "votomatic" pages, voter education appears to be the only antidote.

When the number of candidates for an office is very large, both sides of the card may need to be used for the office. In rare cases, e.g., for voting for delegates to certain national party conventions, more than one card may be needed. In the latter case, all cards for the office from a single voter must be kept together, to identify overvoting.

Processing of multiple cards: When more than one "datavote" card is issued to each voter, more time must be allotted for processing the cards than for a single card per voter, or extra card reader capacity must be added.

3.5 Voting With A Mark-Sense Ballot

With this type of ballot, the voter makes a mark in a small rectangle or circle on a ballot to indicate a vote, and after the ballot is handed in, it is automatically read. Sensing systems originally employed electrical conductivity to determine if a mark had been made, but it is now much more common for light to be used. Thus, the system is often referred to as "optical scan," and is currently used by about seven and one-half percent of registered voters. Mark-sense technology is widely used also in standardized testing, for example for college entrance, and in statewide lotteries.

In the use of light as a sensor (or other part of the electromagnetic spectrum, such as infra-red), the beam impinges on the voting location, and the quality of the reflection of the beam is used to determine whether or not a mark is present. With the system employing infra-red, the voter is not limited to any particular writing instrument or pencil hardness, provided that the mark is not colored red.

Mark-sense ballots are typically not designed in the size, proportions, or thickness of the standard punch card. In most cases, they are larger, in order to allow for the printing of candidate and issue choice information directly on the ballot, while retaining just a single sheet as a ballot. As with the "datavote" punch card, separate blank lines may allow for write-in candidates. A numbered stub should be attached when issued, to permit proper accounting. No special holding device is required for use by a voter.

3.5.1 Vulnerabilities of Mark-Sense Ballot Systems

Mark-sense ballots, like punch card ballots, have the same potential for ballot manipulation frauds as paper ballots, and the same administrative controls may be applied as countermeasures.

Ballot-reader and ballot requirements: As with punch card ballots, accuracy of the reader is fundamental. The reader must be sufficiently sensitive to read the marks without being too sensitive so as to mistake smudges for votes. Similarly, if ballots are automatically fed, readers must be designed so as to transport only one ballot at a time. Jams of ballots in the reader must be adequately dealt with to assure accurate counting. Furthermore, printing of the basic control information (timing marks and voting locations) on the ballot must be precise. The needed precision may increase printing costs.

Treatment of reader-rejected ballots: Some mark-sense readers appear to have a problem in reading a fraction of the ballots (they provide a "go-no-go" indication) without any differences between the read and unread ballots being obvious to an observer. Ballots given a "no-go" indication by the reader may be separated by the mechanism and returned to the input, to allow for reentry. Rules for treatment of ballots unreadable by machine should be instituted to ensure that each voter's choices are counted, if the voter's intent can be determined (see section 4.9 for a pertinent example).

A positive feature of one reader implementation is that it returns the uncounted ballot to the voter if the voter has overvoted any office, thereby giving the voter a chance to eliminate the overvote.

3.6 Precinct Versus Central Count For Machine-Readable Ballots

While voting on punch card and mark-sense ballots is carried out at precinct locations, counting of the votes may be done either at the precincts or at a central location. When voting with machine-readable ballots first started, there were no micro-computers, and all counting was done centrally. With the development of inexpensive small computers not requiring a special environment, the possibility of precinct counting of ballots became viable.

The selection of precinct versus central count is often a political decision, in which the desire for local control and decentralized decision-making is traded off against the higher costs for procurement, maintenance and support of many small machines. Local control appears to be important where there are strong neighborhood political organizations that believe that producing the tally locally, hopefully one that favors their party, assists in attracting committed individuals to the cause. The ability to see the tally produced and carry it to the central summarization location is seen as a reward for precinct service.

With counting at the precincts, unofficial results, obtained from a small removable storage unit of each machine, may be transmitted over telephone lines or hand-carried to the central location, thereby providing a rapid indication of the local outcomes. Los Angeles County, the largest local government jurisdiction in population, continues to use central counting, while Chicago, among our largest cities, uses precinct counting. In Chicago, summarized precinct results on removable data storage devices are hand-carried to regional centers, from which the data is transmitted over phone lines to a central location.

3.6.1 Vulnerabilities of Precinct Count and Central Count

The selection of precinct count or central count is a trade-off in vulnerabilities, as well as in other factors.

Central count: Uncounted ballots must be transported to the central location. The transportation of the ballots is an insecure process requiring effective controls.

The centralization of counting provides additional vulnerabilities, in the possible mixup of ballots from different precincts, and in computer operations. Often, a "header" card is added to the top of each precinct deck of ballot cards to be read. The use of "header" cards implies that the complete instructions to the computer are not already in the program, but are partially provided by these cards. Thus, it is important that the "header" cards, as well as all operator instructions to the computer, become part of the official records of the election. Backup computer components must be available to prevent total breakdown in a central count system. (See section 4.11 for an example of a partial breakdown.)

Precinct count: Machines have to be transported to precinct polling places at least one day before an election. These locations are relatively insecure against a motivated and dedicated adversary. At the polling places, there must be concern to prevent tampering as well as theft. A precinct-located machine usually has an EPROM (erasable, programmable read-only memory) that is inserted in it to specialize the machine for the particular ballot conditions in that precinct. Particular care must be taken to protect the EPROM against tampering, removal, accidental interchange with another EPROM, or replacement with an EPROM containing incorrect data. The EPROM may be attached with a seal to make tampering more difficult, and the EPROM may have data on it which will make it operative only if it is inserted in the machine for which it is intended.

Transmission of precinct results over telephone lines to a central location is a potentially inaccurate and insecure process requiring consideration of controls. Transmission of results needs no special security if only unofficial and summarized results are transmitted after the polls are closed, and connections are made only from the central station outwards. Encryption should be considered if individual choices or summarized results are to be transmitted before the polls are closed, or if the transmitted data is considered to be official. Other special hardware and software controls are required if dial-in connections are to be made. A useful analysis of security controls that may be used is available. [31] To assure accuracy of transmission, provision for parity checks and retransmission in case of error should be included in the communications equipment acquired for this purpose.

3.7 Direct Recording Electronic (DRE) Machines

This type of machine, the newest entry in applying computer techniques to voting, is an electronic implementation of the lever-machine concept. This system type is currently used by slightly more than two and one-half percent of U.S. registered voters.

As with a lever machine, there is no ballot; the possible choices are visible to the voter on the front of the machine. The voter directly enters choices into electronic storage in the machine with the use of a touch-screen, or pushbuttons, or similar devices. If an alphabetic keyboard is provided with the voter-choice entry device, write-in possibilities are significantly eased.

The voter's choices are stored in the machine and summed there with all other voters' choices. At the close of polls, summaries from all machines are then combined to yield final results. (If the machine simply produces a ballot to be reviewed by the voter for correctness, and then the ballots are tallied to produce the final count, the machine cannot be categorized as DRE.)

The determination of the number of individual DRE machines required at a particular location requires the same type of considerations as for lever machines. As a DRE machine essentially consists of a voter-choice entry station and a computer to summarize choices, an implementation using several voter-choice entry devices and one computer is possible. In the latter system, several voters simultaneously use individual entry devices to record their votes. Votes are summarized in a single computer installation that serves all such devices at the precinct.

As with lever machines, overvotes are prevented on DRE machines, but undervotes are permissible. In a typical machine, the voter's choices are entered into a temporary storage unit. The storage unit controls a display, visible only to the voter, of the choices made. With this feedback, the voter is given some reason to believe that the desired choices have been entered correctly into the temporary storage, but no independent proof can be provided to the voter that the choices have, in fact, been entered correctly for the purpose of summarizing those choices with all others to produce vote totals.

3.7.1 Summarization of DRE Machine Results

As a precinct-located machine, a DRE machine may have its results recorded on a removable data storage device or on a printout or both. The printout or device may be carried to a central station, or the data taken from the storage device may be transmitted over telephone lines. As with precinct-located ballot-tallying machines, there must be consideration of accuracy and security controls over such transmissions.

3.7.2 Vulnerabilities of DRE Machines

While the DRE machine is an electronic implementation of the lever machine concept, there is a significant distinction between them, other than their use of different technology. To prepare for each election, each lever machine is separately and individually set up (although several may be set up by the same technician).

Centralization of setup: Each DRE machine in an election receives its EPROM for set up from a single central source (the same as precinct-located ballot-tallying machines). In addition, the instructions on the face of the machine may be similarly produced centrally by computer. This centralization provides the opportunity for added efficiency and elimination of errors in the manual production of large numbers of ballot displays. However, there is the danger that centrally-created errors that are not discovered will be propagated throughout the system.

No audit trail of voters' choices: There is, also, a problem with DRE machines that is not present with ballot-tallying machines. This problem is the verification that the voter's choices have, in fact, been entered for summation precisely as the voter desired. The fact that the voter can see his or her choices on a display, or even receives a printout of the choices made, does not prove that those were the choices actually recorded in the machine to be summarized for generating the results of the election.

The assumption of correct recording of voter's choices must be bolstered with extensive pre-election and post-election review and testing of the logic of the machine, and further assurance that this logic cannot be fraudulently altered after the pre-election test. Furthermore, should this logic fail during the voting process, the logic must have been designed to fail in such a way that the failure is obvious to the voter. Otherwise, the voter will have no chance of ensuring that his or her votes are cast on a correctly operating machine.

Difficulty in operability verification: Pre-election and post-election testing of DRE machines is more difficult than ballot-tallying machines because, like lever machines, data input to a DRE machine is from a human. To statistically test the data-entry correctness of a ballot-tallying machine, a large number of ballots is needed, or a smaller number entered many times may be used. To statistically test the data-entry correctness of a DRE machine, either a person or persons have to vote many times, or a device must be built to simulate the action of a person.

When the voter indicates to the machine (e.g., by pushing a particular button) that the voting process has been completed, the contents of the temporary storage unit are added to the more permanent vote summary storage. Correct operation of the summarization process must be similarly assured.

Some assurance of the machine's correct operation of the summarization process may be achieved by the retention, in a more permanent form, of the set of each individual voter's choices that are determined by the machine. These voter-choice sets have to be retained in randomized locations so that no set of choices can be traced to a particular voter. If individual voter-choice sets are retained, they can serve as insurance against the occurrence of certain difficulties. These difficulties are that the contents of the temporary storage unit may be incorrectly added into the more permanent vote-summary storage, or that the vote-summary storage may be accidentally erased before it can be added to the final totals after the close of polls. The sets of voters' choices on a particular DRE machine may be summarized on an independent DRE machine or general-purpose computer for verification.

With DRE machines, no independently created ballots are available for verification of the correctness of both steps of the vote-tallying process, identified as steps (3) and (4) in section 3.1: precise recording of the expression of each voter's choices, and accurate summarization of all voters' choices to yield final results. Stored voter-choice sets may be used to verify only the latter of these two steps. The machine-produced recording of the expression of each voter's choices is not independent of the machine process that produced it. The machine cannot be used to independently verify its own correctness.

Precinct location: As DRE machines are precinct-located, there must be the same or greater concern for the vulnerabilities of that situation as those listed above for precinct-located ballot-tallying machines. These concerns include the risk of theft, tampering, fraudulent replacement of an EPROM, accidental interchange of EPROMs, and of defacement or alteration of the voting surface. Protection of the internal logic of the DRE machine must be of greater concern than with other types of machines, because of the lack of independently generated ballots.

3.8 Software For Computerized Vote-Tallying

Software that is intended for use in more than one election is usually written in a generalized form, and then is specialized for a specific election. The generalized software may be provided with a set of tables whose values are to be filled in during specialization.

This two-step process may be applied to any form of computerized system: punch card, mark-sense, or DRE. The specialization process establishes the number and names of offices and issues to be considered by the voters, the number of candidates and their names for each office, the number of allowable votes for multiple selection situations, and the implementation of special voting rules, such as for treatment of straight-party overvotes and for crossover voting. When the implementation for which the software is being provided includes precinct-located machines, the specialization process includes provision of the necessary parameters to complete the tables in the software of those machines. A device may be provided that can be used to copy the parameters of the election for each precinct from the main computer into the EPROM of the appropriate precinct-located machine.

Software written for general-purpose mainframe computers may be written in a high-level language such as COBOL. Mainframe computers are likely to be provided with extensive support software, such as compilers and programs for peripheral interfacing. The availability of such support makes the use of a language such as COBOL a reasonable decision. (However, see the discussion in 3.8.1 on "hidden code" in connection with general-purpose computers.) With the advent of single-purpose precinct-located machines having limited support software, much vote-tallying software now tends to be written in assembly language. Assembly language may have an additional advantage in providing the developer with more confidence that the real-time requirements of on-line ballot processing will be achieved by the object code. However, assembly language is considerably more difficult to review for logical correctness.

3.8.1 Vulnerabilities of Software

Vulnerabilities of software include logical errors, the possibility of "hidden code," and undocumented changes. No system type, punch card, mark-sense, or DRE, is immune from these threats. Protection against these threats requires implementation of effective management procedures that assure system integrity and security.

Logical errors: Several categories of logical errors need to be separately considered. First, a distinction may be made between generic logical errors that are independent of the conditions of elections, and election-related errors. Then, the latter may be subdivided into rule-implementation errors and setup-condition errors. Rule-implementation errors concern pre-established voting rules, such as for crossover voting and for straight-party overvotes. Setup-condition errors involve specific election matters, such as wrong rotations and incorrect assignments of candidates to districts.

Generic logical errors: These should be identified and eliminated during qualification testing, in preparation for State certification. Qualification may be done once, by a national testing laboratory, to satisfy the requirements of many States. Ideally, qualification should include a test of all possible features and functions and combinations of them. Resource constraints may limit testing to only some of the possible combinations of program features for a system. Qualification testing may involve review of logical flow charts and specific program code, as well as determination of system response to the normal flow of ballot data. Additionally, responses may be evaluated against the input of incorrect data, special cases, large volumes of data, and unplanned hardware failures while processing. Guidance in planning computer software acceptance testing is available [32], [33].

Rule-implementation errors: Qualification testing requires evaluation of the software as it will be implemented, so that elimination of rule-implementation errors should be a byproduct of this activity. A particularly difficult type of rule to implement is the required restriction in some States to one vote per candidate per voter in a vote-for-two situation when a candidate is listed on two party lines for the same office. Should a voter attempt to vote for the same candidate on both party lines in this situation, an incorrectly implemented DRE, punch card, or mark-sense system may assign the candidate two votes. An example of an occurrence of a rule-implementation error for straight-party overvote is given in section 4.4.2.

Setup-condition errors: Elimination of setup-condition errors is necessary as an activity in pre-election system checkout. In precinct-count systems, it is important to verify that the computer is implemented for the same rotation and other setup conditions as seen on the ballot for that precinct. In central-count systems, testing the system against a large number of ballots or ballot images may bring to light the presence of setup-condition errors. In any system in which there is ballot rotation, it is important to assure that the summarization of each candidate's votes is correct, considering the different ballot position of the candidate in the various precincts. See section 3.8.2 for additional automation that could alleviate the problem of setup-condition error.

"Hidden code": This term refers to a secret computer program inserted into another program provided to an unaware user. Software that contains such hidden code is often called "Trojan horse" software. Hidden code that has a function of copying itself into a user's program and being transferred elsewhere to repeat its intent is often referred to as a "computer virus." The purpose of the hidden code may be malicious, or it may be used to demonstrate the prowess of the perpetrator, or to surreptitiously record information for later retrieval.

Assuring the absence of any hidden code within a vote-tallying program is essential to system integrity; it should be a part of the qualification process. The task may be assisted with the use of a software engineering tool that identifies the use of each path in the program during program execution. If, in the exercise of a vote-tallying program, a particular path is not used (because the conditions that select it have not been employed), such a path may be further investigated to determine the selection conditions.

The problem of finding hidden code is complicated when vote-tallying software is mounted on a general-purpose computer. Hidden code may have been initially placed in a support program of the computer, for example the compiler or operating system. Such hidden code may be activated when the support program is called from the vote-tallying program. If a clock could be accessed by the hidden code, activation could be arranged to occur at a particular time on a particular day. The identification of the presence of such hidden code could be difficult and time-consuming, and a deliberate search, without specific evidence that the code exists, could be impractical.

Assuring system integrity with management controls: Realistic protection against the presence of hidden code in a general-purpose computer installation involves the application of management controls over the installation. An important control for protection against hidden code is the requirement that software be supplied only from an original manufacturer who is known, reliable, and can be held accountable. The copying of software from secondary sources should be forbidden.

Modifications to software must be strictly controlled to prevent unauthorized changes. Restrictions must be in place to control access to program codes that have been approved for operation. Authorized changes should be documented. Previous versions of revised software should be retained according to established procedures. Due to the threats from "hidden code," computer programs have been written that protect against it. The protective program is intended to run with an application, and to identify any modifications that are made. However, it is necessary that the application be initially free of any "hidden code" because only subsequent changes can be identified. In addition, the protective program might not be able to prevent unauthorized modification of computed data that is undertaken during operation from outside the program, for example, from the operating system.

An additional strategy to protect system integrity in vote-tallying is to have the vote-tallying software provided by its developer with all necessary support software, including the operating system, as a complete package. No other software would be necessary. In this way, the complete software for vote-tallying is separated from the influences of all other software. It is common practice for software for precinct-located machines to be provided in this condition. In the future, States may require the complete package of software (for any type of vote-tallying system) to be deposited with the chief elections official or an escrow agent, so that the provision of a complete package of software is responsive to this anticipated request.

The provision of a complete software package enables an additional protection to be applied: the data authentication code (DAC) [34]. This code value, a binary number, is computed by first randomly selecting a certain key value, and then applying that key and a specific mathematical function to the software package. The key value is kept secret. The computation of the DAC (which contains the same number of bits as the key) protects the software against both accidental and intentional, but unauthorized, data modification. To apply the function, the software package is treated as if it were a digitally-encoded message, as the DAC was developed to authenticate messages transmitted over communication lines. In application, the DAC would be generated for the original software deposited with the State, and would be generated also for the supposedly identical software used in an election. The two values of the DAC will be identical if the software packages are identical. (The software to be used in an election would have to be compared with the master copy before subsequent specialization for the election.)

There is a very small possibility that other software packages will have the same DAC value. If the software were altered, the probability of the DAC being the same for the altered software is extremely small. In fact, the probability is inversely proportional to the binary power of the number of bits in the DAC. That is, with an increase of one bit of length in the DAC, the probability of identicality is halved. Typical lengths of the DAC are from 32 to 64 bits. Furthermore, altered software could not be designed to have the same DAC value unless the persons performing the alteration knew the secret key used to create the DAC.

Assuring system security: Provision of all software as a complete package implies that the computer on which the software is to run can be dedicated to election operations. With the wide availability and downward cost trend of minicomputers and microcomputers, this possibility is reasonable, even for smaller election administrations.

The advantage of a dedicated computer is that access to the computer installation may be restricted by the election administration. Controlled access implies restrictions on electronic access to files through terminals or modems as well as restrictions on personnel entry to controlled areas. Sources of hardware, software, and supplies that are used may be controlled to assure accountability, as mentioned above. When the election administration simply serves as one of many users of a general-purpose installation, such restrictions enforced by the election administration are not generally available. The election administration may not be able to assure that the special concern for security necessary in election operations has the same or higher priority in the general-purpose installation.

3.8.2 Integration of Administrative Software

It is now possible to integrate vote-tallying software with other software that relates to the management of elections. Software can be provided that assists in the establishment of districts and precincts, and in the assignment of specific residence addresses to specific precincts. To be most effective, this software would need to be used in conjunction with computerized lists of all streets, street intersections, and established mailing addresses in the jurisdiction. The vote-tallying software would not need to be combined with the election management software, but would require the capability of being able to receive data from it, for example, through the use of shared storage.

Election management software can be used that helps establish ballot configurations and ballot rotations, and therefore can be used in connection with the production of ballots (for "datavote" and mark-sense systems), ballot pages (for "votomatic" systems), and ballot displays (for DRE systems). Such automation should assist in the reduction of setup-condition errors such as rotation errors and candidate mis-assignment errors. Setup-condition error is a major category of administrative error in election management.

In metropolitan counties with a ballot rotation requirement as well as with many overlapping minor jurisdictions, such as incorporated places, school districts, state legislative districts, and judicial districts, the number of different ballot styles in a consolidated election may be very large. Los Angeles county employs about 1800 styles, while other urban counties may use between 200 and 600. (Consolidated elections, involving Federal, state, and local offices simultaneously, have been mandated in many places to reduce costs and improve voter participation.) Computer programs can assist in reducing the need for multiple entry of the same data, and in sorting out the ballot requirements of each precinct and district.

3.9 Local Conduct Of Elections And Distribution Of System Types

3.9.1 The Number of Major Election Jurisdictions

Each jurisdiction that conducts a major election (an election for Federal or State officials) must consider the acquisition and use of vote-tallying equipment. Thus, such a jurisdiction would need to consider the information provided above in this chapter. The ability of such a jurisdiction to bring resources to bear on the issues of acquisition and use of vote-tallying equipment may affect its capability to effectively carry out its responsibilities.

The discussion below identifies the jurisdictions that carry out major elections. The data show that there are a large number of small jurisdictions with election administration responsibilities. Application of resources available at the State level may be necessary to provide smaller jurisdictions with the capability to adequate deal with all of the issues of computerized vote-tallying.

In the United States, the responsibility for administration of elections is a State function (although the Federal Government may impose requirements, and has done so). Our only officials elected nationwide, the President and Vice-President, are indirectly elected by the selection of "electors" in each State. In each State, local governments actually conduct the elections for

State and Federal offices, as well as for offices within their own jurisdictions. In 41 of the States, these major elections are carried out at the county level. (In four of these States, certain "independent" cities serve as county-equivalents and similarly carry out these elections.)

In nine States, major elections are carried out in units of government called minor civil divisions (MCDs) by the U.S. Bureau of the Census. An MCD is a first-order division of a county, and only States in the Northeast and Midwest have such units. An MCD may be a municipality (e.g., a city), or it may be another type of jurisdiction. The nine States in which MCDs conduct major elections are Michigan and Minnesota, in which the non-municipal unit is called a township, and the six New England States and Wisconsin, in which the unit is generally called a town (although other names, such as "plantation," "location," and "gore" identify a few units in Maine, New Hampshire, and Vermont).

Conduct of the election at the local level implies that, at that level, voter registration files are maintained, vote-tallying equipment is procured and maintained, voting locations are determined, precincts are staffed, votes are counted, and election results for the jurisdication are produced. In November of each even-numbered year, when there are many Federal, state, and local officials elected, there are a very large number of mini-elections being administered simultaneously. Thus, the report that there were "Challenges in 4 States" [6] to a vote-counting program should be interpreted to mean that there were challenges to particular contests in elections in four local jurisdictions, one in each of the identified States.

There are about 3140 county-level units in the United States, including some 44 independent cities serving as county-equivalents. However, only about 2870 of them conduct elections for State and Federal offices in the 41 states in which counties and county-equivalents perform this function. There are about 7610 MCDs conducting elections in the nine states identified above. In addition, Washington (coextensive with the District of Columbia) and about 19 other cities (including New York and Chicago), not included above as county-equivalents or MCDs, conduct their own elections. Thus, there are some 10,500 local governments conducting major elections nationwide. Some of them are very large in population, e.g., Los Angeles County, and New York City, and some are quite small, e.g., Loving County, Texas, 1980 population 91. These 10,500 local governmental units essentially define the potential for use of vote-tallying equipment for major elections.

3.9.2 Distribution of System Types

The distribution of system types (for precinct use only, excluding use for absentee ballots) has been determined through a nationwide survey taken by Election Data Services, Inc. of Washington, DC [35]. The survey, based on data acquired in the first quarter of 1988, shows the following distribution, according to 1986 registration figures:

Type	% Of Use By Registered Voters	% Of Use By Counties
Paper Ballots	5.9	32.6
Lever Machine	32.9	29.2
"Votomatic" Punch Card	35.9	22.4
"Datavote" Punch Card	4.3	2.3
Mark-Sense Ballot	7.5	5.6
Direct Recording Electronic	2.7	1.7
Mixed	9.8	6.2
Total	100.0	100.0

The "mixed" systems are in counties in which some areas use the "votomatic" punch card, others continue to use paper ballots, and a few use lever machines. The distribution of these systems by voter registration is approximately 45% "votomatic," 45% paper ballots, and 10% lever machines. With this additional data, the percent use of systems by registered voters is as follows:

Type	% Of Use By Registered Voters
Paper Ballots	11.3
Lever Machines	33.9
"Votomatic" Punch Card	40.3
"Datavote" Punch Card	4.3
Mark-Sense Ballot	7.5
Direct Recording Electronic	2.7
Total	100.0

With some 45 percent of voters still not using computerized equipment (still using either paper ballots or lever machines), considerable opportunity for the implementation of new types of systems continues to exist. For example, it may be expected that in the near future registered voters' use of DRE machines will increase a percent or two, primarily as a result of the replacement of lever machines.

3.10 Future Vote-Tallying Systems

3.10.1 Technological Possibilities

With the increasing availability of data transmission over networks of computers and terminals, there is a possibility of online voting through the use of such networks. Even at present, precinct-located devices could be connected to central computers in an on-line mode. Whether this has some benefit greater than its costs is arguable, as results cannot be released before the polls close. Certainly, communications security must be a consideration.

Large single-application networks already in use that are user-oriented are networks for lotteries and for remote banking. Voting requires significantly more choices than a lottery or remote banking. In a lottery, the bettor selects just one or two numbers. In banking, the accountholder typically makes a binary choice of either withdrawal or deposit, selects an account type, and specifies a single amount. In voting, there may be Federal, State, and local offices on the ballot, plus several questions. The total number of contests requiring a voting decision may be twenty or more, and several contests may permit a selection of more than one candidate from a longer list of nominees.

In use of a network for voting, the traffic conditions would be extreme. The network would be used only about twice a year, but when in use, the volume of traffic would be very high. In a presidential election, over one-half the adults in the nation would be expected to use the network for about four minutes each over a twelve-hour period. In Los Angeles County, over 200,000 voting uses per hour in a presidential election would be required. Whether this could be both technically and economically feasible is problematic.

A possibility that may be more economical is the use of an existing network to which voting use is added when necessary, provided that the capability for the volume of use is present. The general telephone network might be utilized through voice response (to advise the voter of the choices) and push-button phones (for the voter to make choices), but again, volume is a strongly limiting factor. Cable television is another possibility, if it can be generally implemented in an interactive mode.

An important requirement in voting is the verification of registration. In remote-terminal banking, verification of accountholder status is typically accomplished at this time with a magnetic stripe credit-type card and a personal number. At point-of-sale terminals, it is common for sales personnel to obtain account status and to debit accounts to an on-line system with the aid of data on the magnetic stripe. (Lotteries have no personal identification requirement for use.) Whether it would be feasible to have such a system, like the one in use for remote banking, for a small number of uses per year by a very large number of persons is also problematic. Conceivably, social security number, driver's license number, or some other permanently assigned number could be used as an identifier. A card for voting might have other uses at public facilities, such as for library withdrawals or parking in public garages.

- The process of remote personal indentification is the subject of research. In the future, if a system with video bandwidth were available (e.g., interactive cable television), remote signature verification could be possible. At present, a precinct official can compare a prospective voter's signature with a computer-stored copy, but computer comparison without human intervention is not yet considered to be sufficiently accurate. With less bandwidth (e.g., the telephone network), voiceprint verification could be employed, but only if that process could be shown to be highly accurate. Again, this application is not considered to be technically feasible, in a general sense, in the immediate future. It is possible that a personally assigned "smart card," a credit-type card with an embedded computer chip, could be used interactively at a computer terminal to aid the process of remote identification.

3.10.2 Political and Social Priorities

The implementation of any system must be in accord with political and social priorities, as well as meet technical criteria of accuracy and reliability. For example, any installed system must meet several basic requirements: equal access by individuals to the voting franchise, verification of registration, the ability to cast a vote in secret without intimidation, and assurance of fairness to opposing parties. The advantage of establishing polling places (as opposed to voting from homes through cable television, for example) is that neutral locations where voting can occur without intimidation are set up. At neutral and public locations, representatives of opposing parties can be present and can watch the administration of the voting process. The establishment of technological access to the voting process that is available to some persons but not to others (because of acquisition costs borne by individuals) may not be consistent with the concept of equal access.

4. SOME RECENT DIFFICULTIES IN COMPUTERIZED VOTE-TALLYING

The following are examples of difficulties that have occurred in the use of computerized vote-tallying, in the years 1980-1986. The purpose of providing these narratives is to demonstrate the types of difficulties that have been recently experienced. These reports provide support for recommendations concerning procedures that can be followed so that other election administrators may avoid similar difficulties. It is not the purpose of these reports to assess or assign responsibility or culpability for the difficulties experienced.

The examples were chosen for several reasons. Four of the situations (Carroll County, Maryland; Charleston, West Virginia; Elkhart County, Indiana; and Palm Beach County, Florida) had been identified in an article in the New York Times [6]. The situation in Dallas had been reported there in a separate article [36]. The remaining situations provide elucidation of particular types of problems and, in addition, reliable information about the situations was made available by authoritative or competent sources.

As in the 1975 vote-tallying report [1],in which examples of reported difficulties were given, the descriptions should be read with the following caution:

It is not intended that these descriptions be the definitive versions of what occurred. No absolute proof can be offered that the events occurred exactly as described. However, reported data have been supplied by named sources on the scene, and exact quotations by participants and observers are given when appropriate.

4.1 Carroll County, Maryland: November, 1984

Carroll is a county of about 100,000 population whose county seat, Westminster, is located about 30 miles northwest of the city of Baltimore. On November 8, two days after the Tuesday, November 6, 1984 general election, and in accordance with the rules of the Maryland State Administrative Board of Election Laws (SABEL), voted punch card ballots from two districts of Carroll County were taken to a neighboring county, Frederick, to be rerun on an independently-managed system. (Similarly, ballots from Frederick County were taken to Westminster to be rerun.) This rerun, in order to verify the original results, is necessary under Maryland regulations before the results may be certified.

It was clear from these reruns that one of the computers used was in error in determining the outcome of a contest between Wayne Cogswell and incumbent T. Edward Lippy, for Carroll County School Board. Manual counts of the votes on ballots from both Frederick and Carroll Counties showed that the Carroll County computer was the one that was incorrect. The initial but unofficial count, made public on the evening of the election, had incorrectly indicated that Cogswell was the winner.

An investigation, undertaken the next day (November 9) by Craig Jester, a county computer program contractor, demonstrated that a wrong utility computer program for reading the ballot cards had been used. After the correct utility program was installed, the results coincided with those obtained manually and with the Frederick County computer. The utility program, named COLBIN, had been previously written by Jester under contract to the county and had been successfully used in the May, 1984, primary election.

The purpose of the COLBIN utility program was to read the voted ballot cards in the "column binary" format used for voting, rather than in a simpler format. At the request of Carroll County data processing personnel and to reduce the price, Computer Election Systems, the vendor of the vote-tallying system, had supplied the system with an elementary utility program that could read cards only in the simpler format. With the simpler format, ballot cards would be required to have a maximum of one punch per column, not an acceptable situation for the Carroll County ballot. Carroll County contracted locally (with Pelorus, whose president was Craig Jester) for the COLBIN utility program.

On Saturday, November 10, the count was rerun (using the vote-tallying system including the COLBIN program). Members of the county Board of Elections and the County attorney were in attendance. The count indicated that Lippy was the winner. On Wednesday, November 14, eight days after the election, the Board of Elections certified the results, naming Lippy.

The cause of the error was reported in the Carroll Sun on Nov. 18, 1984 in an article by Steve Kelly [37]. A more complete explanation was provided in a letter, dated Nov. 26, 1984, from Thomas J. Van de Bussche, Administrator of the Data Processing Center of Carroll County, to Dr. Thomas Lewis, President of the Carroll County Election Board [38]. Mr. Van de Bussche's letter was included in a report submitted by Dr. Lewis on December 5, 1984 to Mrs. Marie Garber, Administrator of SABEL [39].

Mr. Van de Bussche admitted that, in testing an improved vote-tallying system provided by Computer Election Systems, he had inadvertently replaced the production version with a test version that did not include the COLBIN utility program. The logic and accuracy test of the vote-tallying system on Oct. 25, 1984, performed prior to the election in accordance with Maryland regulations, produced results consistent with the test ballots used. None of the test ballots had more than one punch in any column. Therefore, the test ballots did not reveal the error.

In the general election of November 6, 1984, the contest for the school board seat in question was listed in the same punch card columns as a home rule issue. The two contests were listed on different ballot pages of the "votomatic" ballot holder. The combination of votes for a school board candidate and a particular home rule position in the same column created a punch configuration that was not recognized as valid by the elementary utility program. As a result, some valid votes were not recorded in both the school board and home rule issue contests. Most of the votes not recorded (about 13,000) were for Lippy, because many Lippy voters chose the home rule position listed in the same card column. Votes not recorded on the home rule issue did not affect the ultimate outcome for that question. If the COLBIN utility program had been used, all votes on the contests would have been recognized as valid.

In summary, the incorrect announcement of the result of the school board contest on election night was due to mistakes by the Data Processing Center of Carroll County in using the wrong utility program and in using a perfunctory logic test that did not disclose the problem before the election. No factual evidence is available that contradicts the documentation submitted to Mrs. Garber by Dr. Lewis and Mr. Van de Bussche.

The incorrect announcement was not due to any error in the vote-tallying computer system supplied by the primary vendor, Computer Election Systems, nor any activity undertaken by its representatives. Nevertheless, on July 29, 1985, the New York Times, in referring to this particular situation, reported that "The vote counting program that has been challenged in .... Maryland was developed by Computer Election Systems of Berkeley, Calif." [6]

The error was discovered after the election but before certification because of a Maryland regulation that required recounting on an independently managed system. This specific regulation was based on a recommendation that "further confidence in the machine-counted results can be achieved if mandatory machine recounting of a percentage of the precincts for each race is carried out on a different, independently managed computing system than that used to produce the official count." [40]

On June 11, 1985, another recount of the school board race in question was carried out, using the Carroll County computer, again including the COLBIN program. This recount was undertaken at the request of the State court in which Mr. Cogswell, the defeated candidate, had filed a suit asking that the results of the election be re-examined. The recount verified the correctness of the election results certified on Nov. 14, 1984, although Mr. Van de Bussche has indicated that the recount results did not exactly match the count reported in the certification.

Mr. Van de Bussche has stated that the recount, carried out with all sides in attendance, was hurried and less than precise in that, with the permission of the court, card reader "checks" were ignored in the ballot-reading process. Usually, a card reader "check," indicative of a reading failure, would result in a decision to re-read the entire precinct of voted ballot cards. Instead, the card or cards causing the "check" remained unread and the reading process continued. The failure to re-read an entire precinct upon occurrence of a read "check" resulted in a small but random reduction of votes to both candidates, according to Mr. Van de Bussche. The differences were not significant enough to raise reasonable doubt as to the correctness of the certified results.

According to a July 11, 1985 story by Chris Guy in the Carroll County Times referring to the court-ordered recount, "...defeated candidate Wayne Cogswell had verification that use of an incorrect computer program caused a nearly 13,000-vote mistake in the unofficial totals released election night." [41]

4.2 Charleston, West Virginia: November, 1980

The following discussion was developed primarily from newspaper articles in the Charleston Daily Mail and Charleston Gazette.

Following the general election of November, 1980, three defeated candidates charged gross violations of election laws in Kanawha County, the county in which Charleston is located. Defeated U.S. Representative John Hutchinson first filed a complaint with the U.S. Department of Justice alleging that his civil rights had been violated. The other defeated candidates who joined Hutchinson in charging election law violations were former State Delegate Leonard Underwood and former Kanawha County Commissioner William Reese. Underwood, who was the first to initiate a suit, had filed for a recount after he was edged out in the election by Delegate John M. Wells. (Underwood was re-elected as a State Delegate in 1982.)

According to an article on June 2, 1981 in the Charleston Gazette [42], Darlene Kay Dotson, an employee in the office of the County Clerk, had stated in a deposition taken for Underwood's suit that the ballots from the election in question had been run through the computer on the day after the election to get "precinct-by-precinct reports." According to law, the ballots are to be secured for the official canvass, which was not done at that time. Two members of the County Commission, Robert Silverstein and Al Shepard, each possessed the only key to separate padlocks that were both needed to open the vault in which the ballots were kept, and both denied opening the vault or giving the keys to anyone else to do so.

According to the June 2, 1981 article, Carolyn Critchfield, also an employee of the office of the County Clerk, told Shepard that, to her knowledge, the ballots hadn't been out of the vault before the canvass. "Shepard said Mrs. Critchfield believed Ms. Dotson had events confused with the primary election when the ballots were run the day after the election," the article reported.

There was also concern about a test run of the computer's tabulation ability. Ms. Dotson had testified, according to the newspaper article, that neither County Clerk Margeret Miller, nor the county commissioners would sign the certification approving the test, and that she had to sign it.

Mr. Underwood had filed for a recount on December 2, 1980, and then, on December 16, he asked the circuit court to require that the election ballots be manually counted to compare them with the computer tabulation. In early February, 1981, a circuit judge denied Underwood's request, but on February 17, 1981, he filed an appeal with the state Supreme Court, asking for the manual count or a retabulation by the computer. However, following the circuit judge's denial of Underwood's request, the ballots had been destroyed by order of the County Clerk.

The state law in effect at that time stated that ballots shall be preserved for 60 days and "if there be no contest pending as to such election and their further preservation be not required by any order of a court, they shall be destroyed." According to Ray Dodson, lawyer for the County Commission, Mrs. Miller told him that she did not know that Mr. Underwood had filed an appeal in the state Supreme Court. Dodson said that there is some question as to whether Underwood's appeal constituted a true contest under the law.

On February 24, 1982, according to a February 25, 1982 article in the Charleston Daily Mail [43], County Clerk Margaret Miller was indicted by a special Kanawha County grand jury on six felony and nine misdemeanor charges. Three of the felony charges had to do with the removal of ballots from packages after the unofficial election night vote tally and before the County Commission's vote canvass that produces official totals. Two felony counts accused Mrs. Miller with allowing a vault containing the ballots to be opened between election night and the canvass. The other felony charge stated that she allowed the ballots from the general election to be destroyed while Underwood's suit was pending. In June, 1983, Mrs. Miller was found innocent of all charges. The jury had concluded that there was no "willful misconduct." [44]

However, in February, 1983, the three unsuccessful 1980 candidates filed a civil suit in Federal district court against Mrs. Miller and 15 other individuals. According to a newspaper article on February 5, 1983 [45], the suit alleged that the three were prevented from being elected because of a conspiracy on the part of the individuals named as defendants. In addition to Mrs. Miller, defendants included Mrs. Miller's husband Steven; former U.S. Representative Mick Staton, who defeated Hutchinson in 1980;

Kanawha County Commissioners Henry Shores and Robert Silverstein; Kanawha County Prosecutor (and later mayor of Charleston) James Roark; several employees of the County Clerk's office including Darlene Dotson and Carolyn Critchfield; John Cavacini, Jr., a campaign worker in 1980 for Governor Jay Rockefeller; Computer Election Services, supplier of the electronic voting equipment used in 1980 in Kanawha County; several employees of that company; and Bernard H. Meadows, deputy clerk of the Boone County Commission.

Previous to the filing of the suit, former U.S. Representative John Hutchinson had been reported as charging that one of the defendants, John Cavacini, Jr. was in possession of final returns for the 1980 election two days after the Nov. 4, 1980 election and more than 30 days before the official canvass was completed on December 8, 1980. Hutchinson said, according to a June 5, 1982 article [46], that information in his possession

> "...proves without any question, the machines didn't count at the canvass. I think the results were predetermined. It's conclusive in as much as the documentation shows after numerous absentee and challenged ballots were counted that the totals didn't change. The machine did not count the ballots."

Hutchinson also added that:

> "There is a very great probability that the numbers were in the machine and the machine never counted anything."

In December, 1983, Hutchinson, Underwood, and Reese filed an amended lawsuit that specifically alleged that Kanawha County Clerk Margaret Miller and her staff rigged the vote-counting computers to predetermine the results, that ballots were mishandled, that some ballots were not opened until the canvass and then were counted to meet a predetermined result, that all ballots were not counted, that the vote canvass was falsified, and that the computing equipment was not properly tested prior to the election. The three plaintiffs also claimed that Boone County election officials tampered with the computer equipment before the election, that ballots were altered, and that an accurate ballot tally was not made. Irregularities in procuring the vote-counting equipment in both Kanawha and Boone Counties were also alleged [47].

In May, 1985, the suit was dismissed (charges against several defendants had been previously dropped), and the Charleston Daily Mail editorialized on May 3, 1985 as follows:

> "[U.S. District Judge Charles] Haden sat through days of non-evidence on behalf of three plaintiffs -- former

> Congressman John Hutchinson, House of Delegates member Leonard Underwood and former county commission candidate William Reese -- all of whom lost election races in 1980 and have been mad about it now for more than four years.
>
> "The plaintiffs were somehow allowed to bring this petty case to trial. Throughout, they failed to present a particle of proof to support their claims that 11 defendants conspired to deprive them of public office.
>
> "People who run for election obviously like to win, but they must be prepared to lose. And barring solid evidence of fraud, they ought to accept their losses graciously without proceeding to harass either the individuals who ran against them or those who counted the votes." [48]

Appeals of the dismissal were similarly dismissed, and the U.S. Supreme Court announced on February 24, 1987 its refusal to hear the case.

Possibly influenced by Underwood's initial suit requesting a manual recount of the ballots, West Virginia amended its law on electronic voting systems in 1982. The revised subsection 3-4A-28 (4) is as follows:

> During the canvass and any requested recount, at least five percent of the precincts shall be chosen at random and the ballot cards cast therein counted manually. The same random selection shall also be counted by the automatic tabulating equipment. If the variance between the random manual count and the automatic tabulating equipment count of the same random ballots is equal to or greater than one percent, then a manual recount of all ballot cards shall be required. In the course of any recount, if a candidate for an office shall so demand, or if the board of canvassers shall so elect to recount the votes cast for an office, the votes cast for that office in any precinct shall be recounted by manual count.

4.3 Dallas, Texas: April, 1985

In the election for Mayor of Dallas, held April 6, 1985, the incumbent Starke Taylor avoided a runoff by obtaining slightly more than the required 50% of the vote. There were three opponents to Taylor: Morehead, Goldblatt, and Daniel. Max Goldblatt, the leading opponent, requested a recount. A machine recount (including absentee ballots that were mixed in) was undertaken on April 11, 1985, by order of the District Court. The original results and the recount results are summarized below: [49]

	Morehead	Taylor	Goldblatt	Daniel	Write-In
Original	2,318	38,998	35,081	621	10
Recount	2,318	38,973	35,082	619	10

The machine recount showed that, overall, Taylor's votes decreased by 25, while Goldblatt's votes increased by just one, an insufficient change to cause a runoff election. Mr. Goldblatt did not raise a challenge to the accuracy of the recount at that time, and Mr. Taylor was confirmed as Mayor for the two-year term.

Taken as a whole, the recount results would appear to confirm the vote totals produced in the original count, but a precinct-by-precinct review [50] raises technical questions about the accuracy of the combined human and computer system that produced them. There were 250 precincts in this election, but only 89 precincts showed no change in votes for any of the four candidates in the contest for mayor. Taylor's votes changed in 100 of the 250 precincts, while Goldblatt's votes changed in 113 precincts.

In the recount, Taylor lost one vote in 45 precincts, two votes in each of ten precincts, three votes in each of four precincts, and five votes in each of two precincts. Taylor gained one vote in 25 precincts, two votes in each of nine precincts, three votes in each of three precincts, and five votes in each of two precincts. These changes sum to a loss of 25 votes.

Goldblatt lost one vote in 47 precincts, two votes in each of five precincts, three votes in each of two precincts, four votes in each of two precincts, and five votes in each of two precincts. Goldblatt gained one vote in 41 precincts, two votes in each of ten precincts, three votes in each of three precincts, and twelve votes in one precinct. These changes result in an overall gain of one vote.

In addition, the number of ballots counted changed in 109 of the 250 precincts, for a total loss of 27 ballots [51]. Fewer ballots were tallied in 59 precincts, while more ballots were tallied in 50 precincts. In precincts that lost ballots, one fewer was counted in 37 precincts, two fewer in each of eleven precincts, three fewer in each of seven precincts, four fewer in each of two precincts, five fewer in one precinct, and seven fewer in one precinct. In precincts that gained ballots counted, one more was counted in 33 precincts, two more in each of 13 precincts, three more in each of two precincts, and four more in each of two precincts.

For the recount, data on changes in precinct vote totals for the candidates were made available to the public. However, the number of ballots counted in the recount in each precinct was not included in the data released. The changes in ballots counted that are presented above are based on data collected by Ms. Terry Elkins, campaign manager for Max Goldblatt. Ms. Elkins was present at the recount, and copied down the number of ballots tallied for each precinct.

The causes of the changes in ballots and votes counted are not clear. However, changes occurred in such a manner as to yield both positive and negative values in approximately equal amounts, and the number of precincts in which changes occurred tended to decrease as the value of the change became more severe. This situation suggests a problem of system inaccuracy, rather than of deliberate bias. This inaccuracy could be of either human or mechanical origin, or both.

When numbers of votes change in a system using pre-scored punch cards, the problem is often ascribed to hanging chad, although failure of the card readers to read the cards accurately is a reasonable possibility. If the problem is said to be due to chad, the explanation is that a hanging chad may fall out, creating either a vote or an overvote; or, a hanging chad may be pressed back into place, usually eliminating a vote.

The cause of changes in ballots counted is more perplexing. In the system used in Dallas, ballots were hand-fed into the card readers one at a time, by both the voters and the recounters. Consequently, it is unlikely that, on several occasions, two cards were fed at one time and counted as one. However, the system used at the precincts by voters required each voter to handle his or her ballot twice. First, the voter fed the ballot into the precinct ballot computer. Assuming that the computer accepted the ballot, the voter was then supposed to retrieve the ballot from the output of the computer and drop it into a ballot box. In some cases, a voter may have put the ballot into the ballot box without first having fed the ballot through the computer, or conversely, the voter may have fed the ballot through the computer more than once. On the other hand, inaccurate card counting by the machines, due to card jams, is a possibility. Only a thorough audit of voter sign-in lists, compared with an accurate count of numbers of ballot cards delivered from the precincts to the election headquarters could provide a more confident basis for a statement of the cause of the identified ballot count discrepancies.

In September, 1986, Ms. Elkins concerns about the election were publicized. These concerns included matters other than the differences between the original count and the recount, as discussed above. Instead, a major aspect of the information provided by Ms. Elkins at that time concerned the total number of ballots cast for Mayor. She noted that the "Combined Canvass Report" produced by the Dallas County Election Department on the evening of April 6 stated on page 14 that there were 78,398 ballots cast, while the same document stated on page 27 that there were 80,208 ballots cast. Furthermore, the "Official Cumulative Report" (which serves as an overvote-undervote report), produced by the Election Administration on April 8, stated that there were 79,783 ballots cast. Ms. Elkins contended that documentation that she had gathered supported none of these numbers of total ballots cast.

Ms. Elkins also noted another apparent discrepancy in the results reported for a City Council seat. In that situation (District 7), the number of votes tallied was reported to be 10,365. This value exceeded the number of ballots reported to be cast, 9,679. In addition, in one precinct, the initial number of ballots cast, 263, was replaced later with another value, 515. These technical concerns of Ms. Elkins were supplemented by concerns that the results presented on the computer printouts were created independently of the actual totals of the voted ballots through a deliberate attempt to subvert the outcome. [52]

As a result of Ms. Elkins' complaints, it was reported that Attorney General Jim Mattox and Secretary of State Myra McDaniel began investigations into voting discrepancies. According to the Dallas Morning News of Sept. 23, 1986, "the probe centers on allegations that computerized voting equipment and computer programs used to tabulate state and local elections may have been tampered with to bring about `preprogrammed' results." [53]

In that same newspaper article, Ms. Elkins was quoted as saying that "the allegation is that the computer used to count the votes was given new instructions after it calculated that Max Goldblatt was leading Starke Taylor by 400 votes." Ms. Elkins has noted that the Dallas County computer had encountered difficulties shortly after 8 p.m. on election night, and that the candidate who was leading at 8 p.m., prior to the computer difficulties, was not leading when the computer reported again.

Ms. Conny McCormack, Dallas County Elections Administrator, admitted that the documentation for the April 6, 1985 election could appear contradictory. Her explanation was that the difficulty concerned the treatment of "split precincts," that is, those precincts bisected by the Dallas city boundary. There were 11 such split precincts. The value of 78,398 for ballots cast was produced by assuming zero ballots cast from these split precincts. The value of 80,208 for ballots cast was produced by adding the total ballots from the split precincts, including ballots cast outside of the city. The final value of 79,783 for ballots cast included only those ballots cast within the city of Dallas. Ms. McCormack contended that the recount generally confirmed the correctness of the originally reported outcome. [54]

Ms. McCormack's explanation of the problem of reporting split precincts was supported by the vendor of the vote-tallying system. In a memorandum on the subject, a vendor representative stated that there was a difference between the type of reports requested by Dallas County Elections Department for the PBCs (precinct ballot counters) and for the central computer. The central computer was used to accumulate totals reported by the PBCs. The coding for the central computer included provision for split precinct specification of ballots cast, but the coding for the PBCs did not allow for this. According to the vendor, "this extra statistical option was not requested by Dallas for that election." [55]

The vendor representative further stated, in the same memo, that:

> "Since the [data] packs did not have this [split precinct] information to transmit, all of the precincts which were transmitted had a "zero ballots cast" for the districts. Again, total ballots cast and all candidate votes were present and correct.
>
> "On the cumulative report, then, the votes received by the district candidates were much greater than the ballots cast figures for those districts. Although the explanation for this apparent anomaly is now clear, it clearly was a suspicious looking situation."

With regard to the change in ballot totals reported for one precinct, Ms. McCormack stated that this was due to a failure of a PBC data pack. This occurs about 2% to 4% of the time, she stated. The procedure when this happens is as follows:

> "When [a failure of a PBC data pack] occurs, the actual ballot cards are counted at the central counting station. Such discrepancies from PBC tape to actual ballots cast is determined by examination of the specific Ballot and Seal Certificates. When there is a discrepancy between number of persons signing the signature roster at the precinct and the number of ballots cast according to the PBC tape, then the ballots from that precinct are counted centrally." [54]

A summary of the ballots cast in this election, as officially reported, is shown below, by district. It can be seen from the table that the largest component of ballots from split precincts occurs in District 7, where the increase from Column A to Column B is 1,661. However, 422 of these ballots were from outside the city, so that the total number of ballots cast in District 7 inside the city is 10,918. The latter number is shown in Column C, and it is appropriately higher than the total votes for candidates in District 7, which was 10,365. [56]

District	(A) Excluding Split Precincts	(B) Including All Ballots From Split Precincts	(C) Only Ballots Cast in City
1	9371	9395	9392
2	6314	6314	6314
3	16351	16382	16382
4	14529	14529	14529
5	13088	13088	13088
6	4118	4118	4118
7	9679	11340	10918
8	4948	5042	5042
Totals	78398	80208	79783

Certain technical problems raised by Ms. Elkins seem to have been given a credible explanation, on the basis of information made publicly available in late 1986. However, as Warner Croft stated in his testimony to the Texas House of Representatives Committee on Elections:

> "There is an audit trail but there are holes in it. The audit trail should consist of everything from the ballots themselves to the console log being printed by the computer on election night. The present laws don't identify what the minimum requirements are, so that, with the absence of a minimum definition, it just does not exist. You go after these things, and the laws don't require that they be kept on file now, so they have been destroyed months ago. So you really couldn't tell if there was fact to these allegations are not. That has been one of our problems. Records aren't available; there are no auditable results." [22]

Ms. Elkins' charges that the results were "preprogrammed" independently of the actual votes cast were not put to rest in 1986. In March, 1987, the Texas Attorney-General's office asked the District Attorney of Dallas County to assist in reviewing the election complaints. The review concerned "the reliability of Dallas County's computerized election system and whether the equipment is vulnerable to fraud through subtle changes in computer programs." [57]

On October 14, 1987, the office of the District Attorney of Dallas County replied to the Texas Attorney General's Office with a letter [58] including the following:

> "We have carefully considered each of the thirteen (13) "discrepancies" discussed in the report [submitted by your office], and ... each of the "discrepancies" has been explained to our satisfaction; and although we verified that a few coding errors were in fact made, we

> have concluded that they were the result of unintentional "human error." We find no evidence whatsoever to indicate any deliberate fraud in the 1985 election, nor do we find any credible evidence to indicate an attempt to manipulate the election or its outcome by anyone, be it candidate, election official, or vendor."

Some knowledgeable persons have found this statement puzzling, in view of Warner Croft's testimony that necessary documents constituting the audit trail had been previously destroyed.

In the April, 1987, mayoralty election, split precincts were eliminated by the Dallas County Election Administration. Precincts that had been bisected by the Dallas city boundary or City Council district boundary were divided into two or more separate precincts. Letters A and B, added to the precinct identifier, were used to distinguish the formerly combined precincts, as in 1193A and 1193B.

4.4 Elkhart County, Indiana: November, 1982 And November, 1986

4.4.1 November, 1982 General Election

Elkhart is a county of about 140,000 population on the northern border of Indiana, located about 90 miles east of Chicago. In lawsuits filed in state and Federal courts, several losing candidates alleged that election fraud occurred in the administration of the general election of November 2, 1982.

In this election, the computer facilities of a bank located in the county seat of Goshen were used for ballot-counting purposes. The office of the county clerk had limited computer expertise for carrying out its responsibilities for management of the ballot-counting process. Technical operations related to computer processing of the ballots were undertaken by bank employees and by an employee of the vendor of the vote-counting software. The bank's computer was capable of multiprogramming, and bank operations continued during ballot counting.

It is important to note at this point that punch card ballots in a general election in Indiana have "straight party" punch locations. A voter who votes one (and only one) of these punch locations automatically votes for all candidates of that party unless the voter specifically votes for a candidate of another party in a particular contest. A vote in a particular contest always overrides the straight party vote. This feature of Indiana ballots figures prominently in this situation.

Procedural and computer-related errors in the election affected at least three contests. The errors concerned votes for the Town Board of Wakarusa (a town within Elkhart County), votes for Districts 2 and 3 of the County Council, and votes for a State Representative contest.

The boundaries of the town of Wakarusa are wholly within Olive Township of Elkhart County. Some of the voters in this township live within Wakarusa, and some live outside the town. Only those residing within Wakarusa are entitled to vote for the Town Board. However, no arrangements were made to distinguish town residents from non-residents for purposes of casting ballots. All voters in the township were given the same ballot. The result of not separating ballots of residents and non-residents was that Town Board candidates received more votes than they were entitled to obtain. The extra votes were from voters residing outside the town, and these consisted primarily of straight party votes that were assigned by the vote-tallying computer program to Town Board candidates as well as to other candidates on the ballot. In addition, there may have been votes for individual Town Board candidates by non-resident voters who mistakenly voted for them.

The Wakarusa problem was not discovered until several days after the results were certified, when an election worker realized that the total number of votes for Town Board candidates was much higher than that number of votes which could have been cast by voters entitled to vote for Town Board. The problem was "solved" by an informal agreement approved by the Election Board under which all straight party votes were eliminated for Town Board candidates. This "solution" disenfranchised those voters within the town who lawfully cast straight party votes. The change overturned one outcome, but the loser was dissuaded from suing. According to Elkhart attorney David T. Stutsman, the agreement to change the outcome was in violation of Indiana law, and a legally correct solution would have been to hold a new Town Board election.

In the counting of votes for County Council, votes for candidates in Districts 2 and 3 were interchanged. This situation became apparent to one of the Election Board members when Higgins, the unopposed candidate in District 3, was initially shown to have a significant number of opposing votes. In addition, Barnes, the incumbent in District 2, was getting almost no votes, while Wiedenhoeft, Barnes' novice opponent, was winning a large majority. This unexpected condition was pointed out, and the interchange was discovered. The error was corrected by changes in control cards that were carried out by an employee of the software vendor. This latter individual had been sent from another state by the software vendor for the sole purpose of assisting in ballot-counting operations. He appeared for the first time on the afternoon of the election, and returned to his home state immediately following the completion of the computerized vote-tallying.

In the contest for State Representative, it become apparent late in the evening of November 2 that an incorrect punch position was being used to tally votes for one of the candidates, Philip T.

Warner, in his race against Mike Puro. The software vendor's employee again changed some control cards, and a retabulation was undertaken. The retabulation resulted in a significant change in vote totals: an increase of 3,710 for Warner and a decrease of 53 votes for Puro. The reason that there was a decrease in Puro's totals was because of individual votes for Warner by voters who had also indicated a straight party punch for Puro's party. Before Warner's votes were properly tabulated, the straight party punches had added to Puro's total, but the specific votes for Warner on the same ballots negated these straight party votes.

It seems clear, from the Wakarusa situation, that the full implications of computer processing of ballots were not completely appreciated by the persons responsible for running the election: the Election Board and its employees. In addition, it seems clear, also, from the tabulating errors in the County Council and State Representative contests, that insufficient attention was paid by those responsible for running the election to examination of the "edit list" that identifies, for the computer, the assignment of punch locations to candidates. Adequate testing of the computer system prior to use appeared to be lacking, possibly to an extent inconsistent with Indiana law.

The alleged misfeasances have been described in lawsuit briefs filed by the losing candidates, and documentation on the charges has been obtained from David T. Stutsman, their attorney. A major source of problems in the election was the apparent failure to properly test the equipment prior to use. The losing candidates charged that no test of the automatic tabulating equipment was undertaken five days prior to the election, as required by the Indiana statute then in effect, and that only a superficial test was done at about 4 p.m. on election day.

According to Mr. Stutsman, this test on election day consisted of a count of just 13 test ballots each for only two precincts of the 63 precincts involved in the election. As a result of a lawsuit concerning this election, an alleged configuration of these 13 cards and the results that they generated on the computer have now come to light. According to this information, the test ballots should have generated three lawful votes for the Democratic senate candidate, but instead they generated four such votes. One test ballot that should not have produced a vote contained a straight Democratic punch, and individual punches for both Democratic and Republican senate candidates. A second test ballot that should not have produced a vote contained straight party punches for both the Democratic and Republican parties, that is, an uncountable straight party overvote. One of these test ballots probably supplied the incorrect fourth test vote. If this information about the test ballots and results is correct, the ballot counting process on November 2, 1982 should not have proceeded until the logical error was corrected. As stated in the Indiana statute I.C. 3-2-4-4(f) in force at the time:

> "If any error is detected [in the test], the cause therefor shall be ascertained and corrected and an errorless count shall be made before the automatic tabulating equipment is approved."

Other errors in administration that have been alleged were that the changes in the control cards that were made were not accompanied by system tests, that the computer systems's clock was disabled (thereby preventing times of console actions from being reported), and that no precinct numbers were printed on the ballot cards.

Computer consultants hired by the losing candidates submitted statements including the following:

> "The Edit List was not correct when the program was initiated.... Thorough tests would have caught these irregularities.
>
> "Given the nature of the undocumented program correction ... it is impossible to know exactly how the the program tallied the votes. The control log shows no test of accuracy after the [vendor's] representative modified the parameter cards.
>
> "The lack of a clear audit trail and the lack of error reports, the convoluted code reports plagued with errors, and the unquestioned trust in an untested electronic process seems to be a major problem with this system comprised of hardware, software, and users.
>
> "In the opinion of [the computer consultants,] it would be possible to modify program logic with the use of inserted control cards. It would be possible to change accumulated vote totals by reading in control cards at the appropriate time during the program execution. This would be unknown to the election officials or anyone but an experienced operator. This program uses alter verbs which allows program logic changes with the use of control cards inserted at execution time.
>
> "A knowledgeable operator can change the program logic in execution with insertion of control cards ... many possibilities for change in program logic and vote tally exists." [59]

The losing candidates' case, brought before the U.S. District Court for the Northern District of Indiana, named the local board officials as defendants. It was alleged in the pleadings in that case that the computer system was not tested, that there was no error-free test of the system before the official count, that there was no actual count of the ballots and that the alleged count and certification of the vote count was fraudulent. The pleadings and briefs further stated that the control cards for the operation of the program were altered by the vendor representative during the counting, and that the acts by the election officials were willful, wanton, reckless and oppressive.

However, the court entered a summary judgment on Feb. 21, 1985 against the losing candidates because, in the court's opinion, there were no allegations of any "willful conduct which undermines the organic processes by which candidates are elected" (language of an important precedent, Hennings v. Grafton) [60]. The judgment of the lower court was affirmed by the U.S. Court of Appeals for the Seventh Circuit, which stated that "the appellants (i.e., the losing candidates) confuse fraud with what is at most willful neglect." [61] Mr. Stutsman notes that the plaintiffs were not allowed to present their evidence in the case. The lawsuit was dismissed as a matter of law, without a trial on the merits. Therefore, a jury was not allowed to hear the case.

A second Federal lawsuit, filed in the Southern District of Indiana, continues to be pending, with the vendor named by the New York Times as the principal defendant. This suit charges negligence, breach of contract, and strict liability, alleging that the computer system used in the election was sold in a defective condition and caused loss and damage to the losing candidates. In addition, it is alleged that the vote counting was a fraud and that the certification of the vote totals was false and fraudulent.

4.4.2 November, 1986 General Election

Following the 1986 general election, a State-mandated recount was undertaken that included ballots from Elkhart County. In this recount, directed by Dean David Link of the Notre Dame Law School, it was discovered that the computer program used to count ballots in Elkhart County was not counting correctly according to Indiana law. The problem occurred in the treatment of ballots that were overvoted in the "straight party" positions. According to Indiana law, these ballots should be voided for all partisan contests. Instead, the ballots had been counted in the contest being recounted. These ballots were eliminated in the recount.

4.5 Gwinnett County, Georgia: November, 1986

A recount undertaken in a State Senate race showed the loser in the first count winning the contest by 77 votes. The original tally had given challenger Steve Pate a winning margin of eight votes. However, the recount gave incumbent Donn Peevy 13,682 to Pate's 13,605. According to an article in the Atlanta Constitution, November 13, 1986, "the recount was the result of a computer hardware error ... affecting hundreds of uncounted votes

..." [62] The "computer hardware error" in question was believed to be a problem with the card readers that read the pre-scored punch card ballots.

Allegations raised in this election included charges of "hidden ballots." It appears that a box of ballots and documents received from one precinct was initially believed to consist of the complete set of voted ballots on top of other documents in the box. When the documents were removed from the box after the ballots on top had been counted, more ballots were found under the documents. In addition, it was "charged that ballots from two precincts did not arrive at the elections office until early on the morning of Nov. 5 [the day after the election] in the car of the elections board member," according to the article in the Constitution.

The original count was undertaken on a system consisting of two personal computers, each with a card reader, networked together to drive one printer. For the recount, it was agreed to separate the two computers and to count the ballots twice, once on each computer. Unfortunately, the recounts obtained from the two computers were slightly different, although not of a difference sufficiently large to overturn any contest.

The Georgia Tech Research Institute (GTRI) was asked by the office of the Secretary of State of Georgia to render any possible assistance. GTRI decided to review the situation and to determine the source the discrepancies between the two computer outputs. The investigatory team, headed by Dr. Britain Williams, hoped to separate the causes of the errors into at least two classes: those caused by handling of the ballots by voters and voting officials, and those caused by the hardware. According to Williams, "everything that could have been done to insure the accuracy of the recount was, in fact, done and the discrepancies observed are inherent in this type of system. A thorough analysis of these results will be conducted in an attempt to estimate the inherent error in using pre-scored ballots." [63]

A report has now been produced by Williams and an associate. [106] The report compares differences in the results in three counts: the general election, and the recounts on the two individual machines. The report states that:

> "Errors were either tabs which were not yet dislocated from their pre-punched positions in the ballot, or stray tabs which filled other previously punched-out positions (+ and - errors)."

According to the report, errors were caused by such factors as handling procedures, the ballot puncher (which was of the "votomatic" type), the vote counter, the punched card's density, vote position on the ballot card, human error, and pure chance. The report concludes that:

> "...there should be a system set up to make the voters and especially the volunteer workers aware of the effects procedural care has on the accuracy of tabulations (since this was where the main problem was discovered). Details like not putting large (or any) rubber-bands around the ballots would also be advisable (especially since custom ballot carriers are provided)."

4.6 Illinois - Statewide Testing Program

The Illinois State Board of Elections, Division of Voting Systems, under the direction of Michael L. Harty, (now Director of Elections, Maricopa County, Arizona) has undertaken tests of vote-counting computer systems. Between 1983 and 1987, the division conducted 48 tests of the automatic tabulating equipment and computer programs in 41 election jurisdictions. The tests have involved anywhere from 1,000 to 65,000 test ballots. The division found apparent computer program tabulation errors in 11 of the election jurisdictions tested. The division reports that most of these errors would not have been discovered without adequate testing. As a result of its testing experiences, the Division of Voting Systems has concluded in its Summary of Findings and Observations on State Board of Elections Computer Testing Program, revised February, 1987: [64]

> "The testing of computer vote tabulation systems needs to be improved substantially. At a minimum, voting systems tests must be large; must test all voting positions; must test overvotes and undervotes; column binary punches; straight and split party votes; nonvoting position punches; and must test for every candidate in every ballot configuration in every precinct. Only by extensive testing of a computer vote tabulation system can we be reasonably assured that tabulation of the ballots will be entirely accurate".

The following descriptions of programming, program initialization, and hardware problems in local jurisdictions in Illinois are taken from the reference given above.

4.6.1 Programming and/or Program Initialization Errors

Whiteside County - 1986 General Primary Election: The system tabulated votes on ballots that contained invalid security codes (ballot style identifiers).

Morgan County - 1985 Consolidated Election: No straight party votes registered for the candidates of a party. However, this did not affect the individual candidate totals.

Peoria County - 1985 Consolidated Election: The computer program misassigned straight party punches for a candidate for township supervisor. The candidate received a tally from a straight party punch for the opposite party but failed to receive a tally from the straight party punch of his own party.

Sangamon County - 1985 Consolidated Election: The computer program would not accept ballots with proper ballot style identifiers. This error was not discovered by the test previously run by the local jurisdiction. In addition, ballots in precincts with more than one ballot style did not contain different style identifiers. Thus, it would not have been possible to separate the voted ballots of the different styles.

Logan County - 1985 Consolidated Primary Election: Tabulation errors occurred when precincts were split by ward boundaries. When the same punch position was assigned to different candidates in different wards in the same precinct, votes for one of the candidates were not tallied by the computer program.

Effingham County - 1984 General Election: A county-level office was not being tabulated in five precincts, though votes were assigned to the office.

Jackson County - 1984 General Election: A translation error between precinct returns and the summary report caused the summary report to fail to properly reflect the precinct sum totals for certain candidates.

LaSalle County - 1984 General Election: The straight party vote was not being tabulated for all candidates in a party. In addition, when an overvote occurred in the straight party column and also in an individual candidate's punches on the same ballot, the candidates involved actually lost a vote, i.e., had their vote totals reduced by a vote (instead of simply being denied a vote).

Grundy County - 1984 General Primary Election: Forty-seven percent of the precincts had one or more of the following types of errors: (1) the assignment of the wrong county board districts in the precincts, (2) the deletion of candidates in precincts, (3) the incorrect assignment of candidates to precincts, (4) assignment of only 1/2 vote for each vote cast, and (5) incorrect totals of precinct votes on the summary report for several candidates.

Rock Island County - 1984 General Primary Election: Two votes for each vote cast were being tabulated for a candidate. In addition, the "no" votes on a proposition were not being counted. Further, the summary report totals did not properly reflect precinct sum totals for several candidates.

4.6.2 Hardware and Punch Card Difficulties

City of Chicago - 1987 Consolidated General Election: The system test indicated an approximate 3% failure rate of program chips. The chips were improperly programmed or "burned." The malfunction would have been identified during the public test.

Boone County - 1987 Consolidated Primary Election: Due to substantial ballot quality defects, a system test could not be executed. New test ballots were ordered.

Pulaski County - 1986 General Primary Election: The principal disk that contained the vote-tallying program failed to operate for the system test. The duplicate (backup) disk was employed. The principal disk operated correctly for the public test. No reason for the problem was discovered.

Jackson County - 1984 General Election: Column binary punching appeared to cause severe tabulation delay. In addition, the card reader stopped occasionally during the tabulation of a precinct. When this condition occurred, the results already obtained had to be erased and all the ballots for the precinct had to be retabulated. The cause of this difficulty could not be immediately ascertained.

Will County - 1984 General Election: During the system test, the card reader was jammed twice by ballots. The ballots involved were almost completely destroyed in the process.

4.7 Maricopa County, Arizona: September, 1986

A clerical error that would have interchanged votes for the two major parties in this primary election was caught during testing. Pre-punches (ballot style identifiers) were incorrectly specified, and if the errors had not been caught, votes in the primary contests in each party would have been assigned to the other party during tallying. Poor communication between the county data processing department and the election administration contributed to the problem. A well-designed testing process caught the error, so that ballot counting during the actual election was not affected. [65]

4.8 Moline, Illinois: 1985 Consolidated Municipal and Township Election

The following report is primarily based on an article in Illinois Issues, November, 1985, that was republished in a newsletter of the National Center for Policy Alternatives. [66]

In this election on April 2, 1985, the failure of a card reader to read correctly caused a losing aldermanic candidate for Moline City Council to be put into office. The error was not rectified until about three months later.

The failure of the card reader was not initially apparent. It was only discovered after defeated Moline 3rd Ward aldermanic candidate Earl Wendt went to court to demand a recount. Wendt had lost by two votes, and the recount was ordered by Rock Island County Circuit Court. In the recount on May 14, Wendt picked up two votes, but his opponent Allen McCauley picked up 92 votes. The large change in McCauley's total demonstrated that a serious error in vote-tallying had occurred. The data showed that the error was in the failure of the system to tabulate many straight party votes for McCauley. Further investigation appeared to demonstrate that the problem was a slipping timing belt in one card reader.

As a result of the Wendt-McCauley recount, the party of losing 4th Ward aldermanic candidate Charles Reynolds also demanded a recount in a petition to the Moline City Council. Reynolds was of the same party as McCauley. However, the City Council denied this petition and two similar petitions from other candidates on the basis that the 30 days following the election allowed for such petitions had expired.

Following these denials, Dennis Faust, assistant State's Attorney submitted a petition of quo warranto to Chief Judge David DeDoncker of the 14th Judicial Circuit. The quo warranto petition, whose origin in Anglo-American law goes back to Edward I in 1275, is used to remove "any person [who] shall usurp, intrude into, or unlawfully hold or execute any office...", according to the Illinois Revised Statutes. Faust's theory was that if members of the Moline City Council hadn't received a majority of the votes, then they held office illegally.

On July 8, Judge DeDoncker agreed to a recount for the office of city clerk and for three aldermanic offices including that for the 4th Ward, despite the fact that the 30-day period had expired. He stated that there was no knowledge that a machine was not working until 40 or 50 days after the election. "We had legal American voters who voted and did not get their votes counted", DeDoncker said. The judge appointed representatives of the vendor of the vote-counting system to serve as officers of the court and ordered them to conduct a recount. A judge of a higher court refused to stay the recount, and it proceeded.

As a result of this recount, alderman Roy Lear picked up two votes, but his opponent Charles Reynolds added 135, making the final count 557 for Reynolds to 473 for Lear. Through a court order, Lear was removed from the city council. Reynolds was seated in his place. Lear did not appeal.

4.9 Oklahoma County, Oklahoma: November, 1986

In the general election of November, 1986, difficulties perceived by an independent group of local observers involved, among other items, the operability of the precinct-located, mark-sense computers, and the anomalous numbers of counted ballots that were reported. These observers, David Clampitt, Carolyn Burkes, and Sue Milton, submitted the data on which the discussion below is based.

The county signed a contract to purchase the mark-sense vote-counting equipment in the summer of 1984. The State of Oklahoma has no system of prior State approval of voting devices before such devices may be purchased by a county. However, no county may purchase a type of voting device before the State Board of Elections has implemented rules of operation for that type of device. Four counties in the State utilize mark-sense type voting devices. Oklahoma County is the only county of these four utilizing the particular model in question.

Engineering tests on the particular devices purchased by Oklahoma County were not carried out by the county until November and December, 1984, when the equipment was being delivered. A feature of the equipment noted in the tests was that a certain number of ballots were not being processed (were being treated as unreadable) by the machines. Approximately 1.5% of the ballots were so treated by each of the two different units being tested. According to the report, "non-processed [ballot] cards were not visibly different from those accepted and tabulated, nor were they always the same cards on successive runs." [67]

The vote-counting equipment was used in a special election at about the time of the test, and the report notes that:

> "The frequency of non-processed ballots [5.22%] was observed in several precincts to be significantly higher than that observed during testing. This is attributed to improper insertion of the card by the voter, namely, failure to insert the card vertically and release it cleanly....We attribute this rate primarily to voter unfamiliarity with the system...."

The report recommended that:

> "Although the [vendor's equipment] is judged to comply with all applicable statutes and regulations,....as [one of four] desirable product improvements, the vendor should be encouraged to reduce the frequency of random non-processing of acceptable ballots."

During the November 4, 1986 general election, the number of non-processed ballots was over 2% in a significant number of precincts. According to State rules, the county Board of Elections "has the authority" [68] (but is not required) to recount precincts with over 2% non-processed ballots. The county board has used its discretion in selecting particular precincts for reprocessing. Reprocessing, if done at all, is done on the county's central computer. Not all precincts with over 2% non-processed ballots were reprocessed in the November, 1986 general election.

Ballots that are not reprocessed and read by the central computer would never be counted at all, except under a court-ordered manual recount. There are no State or county rules which would permit non-processed ballots to be counted manually in order to have the manual results added to those results already obtained by machine.

Results of the 1986 general election in Oklahoma County show, in many cases, a lack of reconciliation of the number of voters signed in at each precinct with the number of ballots cast. Table 1 below demonstrates that fact.

Table 1

	Ballots Cast							
Pct.	A	B	C	NP	Total	Voters Times 3	% NP	R
1	1036	1047	1063	104	3250	3261	3.2	
6	513	516	521	20	1570	1557	1.3	R
10	389	396	400	48	1233	1221	3.9	R
34	897	942	976	242	3057	3003	7.9	R
39	1014	1094	1092	168	3368	3372	5.0	
59	370	374	381	47	1172	1173	4.0	
61	37	38	38	4	117	117	3.4	
72	65	71	71	6	213	213	2.8	
82	708	722	775	350	2555	2481	13.7	R
98	380	398	406	46	1230	1284	3.7	
106	546	514	590	201	1851	1857	10.9	
117	22	26	24	7	79	78	8.9	R
122	870	1002	987	350	3209	3126	10.9	R
126	250	257	261	36	804	807	4.5	
131	10	11	11	0	32	33	0.0	R
135	156	284	340	350	1130	1047	31.0	R
136	104	107	109	7	327	327	2.1	R
154	164	186	187	46	583	570	7.9	R
159	663	861	905	489	2918	2820	16.8	R
161	904	948	950	110	2912	2889	3.8	R
202	16	16	17	4	53	51	7.5	
208	116	121	123	14	374	375	3.7	
222	539	578	585	197	1899	1857	10.4	R
256	249	258	266	29	802	807	3.6	
268	682	697	696	51	2126	2154	2.4	
270	953	1224	1319	703	4199	4062	16.7	R

In this election, each voter was given three ballot cards, designated as A, B, and C. The number of processed A, B, and C ballot cards and the number of NP (non-processed) ballot cards are totalled in Table 1 for selected precincts. The total of the ballots tabulated (Total column) may be compared with three times the number of voters signed in at each precinct (Voters Times 3 column), as shown in the table. Values in these two columns in the table for the same precinct differ in most cases. According to a January 25, 1987 article in The Sunday Oklahoman entitled "Security of Elections Described," [69] "an examination of the ballot accounting forms used in last November's election in Oklahoma County revealed that a number of them are neither filled out nor signed." In addition, said the article, precinct voting materials are not logged in on a time sheet when received at the central location, except for the first and last precincts.

The "%NP" column in Table 1 indicates the percentage of non-processed ballots, over all ballots counted. The "R" column indicates whether, as a result of the non-processed ballots, the precinct was recounted on the county's central computer. Several precincts with significant percentages of non-processed ballots were not recounted, at the discretion of the County Election Board.

In most of the precincts identified in Table 1 that were recounted, the total number of ballots counted exceeds the three times the number of voters. From this situation, it may be inferred that the recounting of non-processed ballots (sometimes up to four times in an effort to get them to be read) was not properly accounted, and repetitive attempts at reading added incorrectly to the total number of ballots. The failure to match totals of ballots fed into the machines against voters signed in calls into question the reported individual candidate totals, as no proper cross-foot total can be obtained.

The failure of proper accounting naturally raises the issue of a manual recount. Although there was no request for a manual recount in this election, there have been such requests in other elections in Oklahoma County. It has been the position of the Oklahoma County Election Board that State law, until recently, did not allow manual recounting, since the Board's interpretation of State law is that the same system that was used for the original count must be used for recounting. However, this interpretation has been continually challenged in the courts and has been overturned. There have been manual recounts in Oklahoma County, over the protestations of the Election Board. In the most recent session of the State legislature, a law was passed allowing a recount petitioner to select either a manual recount or a machine recount, in those counties that use vote-tallying devices.

In addition, during the November 4, 1986, general election, over one-third of the 273 voting machines used in the election failed in some manner, some more than once. The most prevalent type of failure was that the machine simply stopped accepting ballots. [70]

Another anomaly of the reported results of this election in Oklahoma County is that the lower-level offices and obscure State questions on the ballot appeared to be as popular with voters as the office of governor. That is, the traditional "fall off" of voter interest in the lower-level offices and State questions did not occur, at least according to the reported results.

This condition is shown in Table 2 below. The votes for the offices of governor, State representative, and on State question #589 are given. The office of governor appeared on ballot card A with other State-wide and Federal offices. The State question appeared on ballot card B, and the office of State representative appeared on ballot card C.

Table 2

Precinct	Votes for Governor	Votes for St. Rep.	Votes for Question #589
1	1025	1039	982
6	509	515	484
10	379	398	359
34	881	941	914
39	989	1032	1038
59	362	367	343
61	37	38	37
72	64	69	69
82	696	not reported	665
98	376	389	351
106	540	581	474
117	21	23	25
122	855	962	918
126	248	255	228
131	10	11	10
135	156	323	258
136	103	106	104
154	162	180	168
159	652	878	808
161	885	927	899
202	16	17	16
208	115	117	117
222	529	557	536
256	246	260	243
268	664	683	631
270	926	1218	1091

In every case in which a vote was reported in the identified precincts, the office of State representative received more votes than the office of governor. In some cases, State question #589, an unimportant issue that would have been expected to receive little public interest, received more votes than the office of governor. Most independent election observers would have difficulty accepting this situation unless a very special condition of strong public concern could be demonstrated.

A commentary on this situation with regard to precinct #270, the last precinct listed in Table 2, was reported by The Sunday Oklahoman on January 25, 1987 in an article entitled "Uncertain Vote Count Puzzling to Analysts." [71] The article pointed out that in demographically comparable Precinct #459 in Tulsa County, the unusual reversal of drop-off did not occur. The race for governor in the comparable Tulsa County precinct received more votes than other races, as would be expected.

4.10 Palm Beach County, Florida: November, 1984

Following the November, 1984, general election, David Anderson, defeated candidate for Property Appraiser of Palm Beach County, sued to contest the election of his opponent Rebecca Walker. [72] Anderson asked that the Court order a hand recount of the ballots, or a hand recount of at least several precincts in that election. The issues on which Anderson sued included handling of the ballots, precinct procedures for signing in voters, ballot secrecy, counting of punch card ballots, and possible manipulation of the computer program. Anderson's initial complaint was dismissed in Palm Beach County Circuit Court on March 1, 1985 [73], but he filed an amended complaint. With regard to the computer-related points at issue, Anderson charged in his amended suit that:

> "There were irregular counts from the computer on each total, each time it was run. The tabs caused by perforations punched in the voting process in the computer cards did not all tear loose, thereby seriously affecting the vote results. It is apparent that because of the type of equipment and method used, that it is impossible to accurately count any election." [74]

Clearly, there were problems of hanging chad ("tabs..[that] did not all tear loose") in this election. In a document filed in connection with this suit (Defendent Walker's First Request for Admission to Plaintiff) [75], the results of a computer recount of another contest in the same election were given. In the other contest, Owens versus Perry, Owens' original total of 137,994 increased by 279 votes in the recount, while Perry's original total of 137,817 increased by 214 votes. According to Ms. Jackie Winchester, Supervisor of Elections in Palm Beach County, these changes were due to chad that were not fully removed in the first count (thereby resulting in no vote) but which fell out before the recount (thereby adding to the original totals). However, no report of undervotes or overvotes is required by the State of Florida or by Palm Beach County, and therefore it is not possible to confidently deduce from the data that this reasonable supposition is correct.

In his amended complaint, Anderson also charged that:

> "The election was run on machines that permit a means of changing the result on the ballots contrary to the votes cast by electors through an alter system in the commands in the computer program, or through the use of a single or several ballot cards specially marked with an alter code on them, which the Plaintiff has reason to believe was activated during the counting of the ballots." [76]

No documentary evidence in support of this claim was filed by Anderson, and in fact, in his initial suit that was dismissed, Anderson had alleged that the election "may have been" run on machines that should not qualify under state laws since "there may be" under the system a means of changing the result through an alter system in the commands in the computer program.

In a motion to dismiss, defendent Rebecca Walker noted that the Department of State of the State of Florida previously approved the voting system in use, and that there is no provision in the Florida election laws allowing for a hand recount of ballots cast through the use of an electronic voting system. [77] The Owens-Perry contest had been recounted by computer two days after the initial count because it was sufficiently close to meet the statutory recount test. The Anderson-Walker contest was insufficiently close to require a recount, but was actually recounted as a by-product of the Owens-Perry recount. The computer recount of the Anderson-Walker contest was unofficial, and the same result showing Walker winning certainly did not satisfy Anderson.

On March 28, 1985, according to Ms. Winchester, a hand count of ten precincts selected by Mr. Anderson was undertaken by the staff of the Supervisor of Elections. Mr. Anderson and his observers were in attendance. "Mr. Anderson and everyone else present agreed that were were no substantive differences", reported Ms. Winchester. On September 10, 1985, Mr. Anderson's amended suit was "dismissed with prejudice" by Circuit Court Judge Richard I. Wennet. [78]

4.11 Salt Lake County, Utah: November, 1980

A last minute breakdown of one of Salt Lake County's two ballot reading computers caused a delay in production of the tally. No county totals were produced for two hours, and the final tally was produced at 5:39 a.m. the following morning. The situation was reported in an article in the Salt Lake Tribune on Nov. 6, 1980. [79]

Although spare parts were available, a decision was made during the count not to attempt to repair the machine, but to keep going with the one ballot computer that was working.

The situation might have been helped if a head start on ballot counting had been implemented, as was done with paper ballots. However, it was believed that this might have created confusion in the meshing of early-collected ballots with the later ones for the same precincts. In addition, no election workers were available to collect the early ballots. It would have cost extra money to hire additional workers, as others were occupied with regular jobs during the day.

It was noted that the complete 100% tally was available much earlier than such a tally would have been available if paper ballots had been used.

4.12 Stark County, Ohio: May, 1986

The following description is adapted from the account given in the July 21, 1986 issue of Election Administration Reports [80], Richard G. Smolka, Editor, with permission of the publisher.

Stark is a county of about 400,000 population whose county seat, Canton, is located about 60 miles south-southeast of Cleveland. An unprecedented court-ordered "audit" (hand recount) of a Stark County computer recount in a county commissioners primary contest again named as winner the candidate who had apparently won in the official results of the May 6, 1986 primary but lost in the computer recount. The "audit" revealed a computer program error that permitted over 100 invalid punchcard ballots to be counted in the recount.

At the end of the election-night count, Robert A. Capestrain held a 26-vote lead in the three-person contest to be Democratic nominee for county commissioner. A recount by computer on May 27 (held because of the closeness of the original tally) put Patty Miller ahead by 5 votes. For the computer recount, the computer program used to obtain the original results was not used. Instead, a special computer program was written, in order to count only the disputed contest and not the other contests on the ballot. The mystery, however, was why 165 additional votes had been tallied in the recount although the number of ballots read by the computer was the same.

The following table provides the votes for the three candidates in the computer tally of the primary, the computer recount, and the hand counted "audit":

Votes Counted for Stark County Commissioner
Democratic Primary Election, 1986

Candidates	Primary May 8	Recount May 27	Change	Audit July 8	Change
Robert A. Capestrain	12,967	13,018	+ 51	12,980	- 38
Donald E. Casar	7,987	8,019	+ 32	7,989	- 30
Patty Miller	12,941	13,023	+ 82	12,952	- 71
TOTALS	33,895	34,060	+165	33,921	-139

The 165 additional votes in the recount were randomly distributed throughout the 481 precincts. Most precincts had no changes, and most of those with changes had a one-vote increase. All candidates gained votes. The names of the candidates were rotated by precinct in the ballot booklets in positions 98-100-102, and the extra votes were distributed among these numbers on the ballot cards. Each of the three positions received approximately the same number of additional votes.

Initially, there seemed to be no satisfactory explanation for the additional votes. Hanging chad was suspected as a possible cause. Fraud was much less likely because it would have required access to ballots from all affected precincts, working knowledge of the ballot rotations, plus sufficient time to locate and punch ballots which had not been voted for county commissioner.

Following the computer recount that indicated a reversal of the initial count, candidate Capestrain filed suit challenging the recount. Because of the unusual nature of the recount result and rumors of fraud, the candidates, attorneys, election board, and court agreed to "audit" procedures that would resolve any identifiable problems with "hanging chad" as well as ensure that the vote count would be complete and accurate. Most importantly, they all agreed that the audit would constitute a final resolution of the vote count dispute. Judge Harold E. DeHoff of the Stark County Court of Common Pleas included a provision in the agreement that all parties would waive any rights of appeal.

The audit included a manual count and a computer count. Forty two-person teams were assigned to manually count the ballots under specific rules. The court order also provided guidelines on removal of hanging chad and specified that only the two master commissioners, appointed by the court, could remove a suspected chad or hanging chad.

Before the start of the audit, Ohio Director of Elections Dorothy Woldorf and area manager Robert Braun of the vote-counting system vendor gave the counting teams both written and verbal instructions on procedures to be followed. The manual recount began at 9:00 a.m. and continued until completion at about 7:45 p.m.

After the first several precincts were manually counted, it became evident that the audit was producing totals more closely matching the original count rather than the recount. By 11:00 a.m., the recount program error had been uncovered. The error was due to the failure of the recount program to distinguish between Democratic, Republican, and unaffiliated ballots.

In the May 8 primary, voters were given Democratic, Republican, or unaffiliated ballots, depending on their party registration. The logic in the computer program and associated header cards that were used to tally the primary ballots was able to distinguish among the different types of ballots, even though all the ballots were tallied on the same computer equipment.

In the recount, all the ballots were again tallied together on the same equipment, but the logic of the recount program could not distinguish among the different ballot types. It was apparently believed by the author of the recount program that the assignment of unique ballot positions to each contest and candidate was sufficient to separate the ballots. However, some Republican and unaffiliated voters had "voted" (i.e., punched out chad) in a ballot position assigned to a candidate in the Democratic county commissioner contest. These ballots were not counted in the Democratic primary tally, but they were counted by mistake in the computer recount.

In the audit on July 8, the ballots were first separated by party before being given to the two-person teams. The separation was easily accomplished because the ballot types were distinguishable by color. Consequently, in the manual recount, "votes" by Republican and unaffiliated voters were not tallied.

During the audit, the master commissioners completed removal of chad on 28 ballot cards. Nine of these were identified as "hanging chad", and the others were termed "bulging chad". One commissioner said that it was obvious that the voter had detached the chad, but that it had been pressed back into position, probably when the cards were stacked. The removal of the chad by the commissioners had no effect on the outcome, but did increase the vote by a net of 26 over the original count.

4.13 Summary Of Problem Types

The problems in specific elections that have been described are categorized below in order to identify the most prevalent types and elucidate the specific difficulties.

4.13.1 Insufficient Pre-election Testing

Lack of sufficient pre-election testing appears to be a major source of operational difficulty. Problems in the following situations would have been avoided if significantly increased numbers of test ballots, using many different expected vote combinations, had been run through the machines and the results compared with expected answers:

* Carroll County, MD; Nov., 1984: A larger number of test ballots, using different combinations of voting possibilities, would have demonstrated the incorrect vote-counting due to the presence of the wrong utility program, and would have avoided the embarrassment and controversy that resulted.

* Elkhart County, IN; Nov., 1982: A larger number of test ballots should have brought to light the three separate coding errors: failure to distinguish Wakarusa voters from other voters in the same township, the reversed tallying in the County Council races, and the incorrect punch position used to tally votes in the State Representative contest. The fact that all three errors were identified after a significant number of votes had been actually tallied (and because the strange results raised suspicions) supports the concept that more test ballots would have brought the errors to light before the tallying began.

* Elkhart County, IN; Nov., 1986: A larger number of test ballots, testing the correctness of the logical rules, would have identified the incorrect logic of the straight party overvote implementation.

* Illinois Statewide Testing Program: The use of a larger number of test ballots would have made clear the logical errors in programming and coding that were identified. This need was recognized by the testers from the State Board. [64]

* Moline, Il; April, 1985: The implementation of pre-election testing might have brought to light the ballot-reader failure before the election, and therefore might have prevented the losing candidate from being certified as the winner.

* Stark County, OH; May, 1986: A more complete checkout using a large number of ballots would have identified the logical error that caused the program used in the recount to fail to distinguish between voters of different political parties.

* A situation not appearing in this category is Maricopa County, AZ. Adequate checkout procedures in that jurisdiction prevented the incorrect punch position assignment from being implemented in the election.

4.13.2 Failure to Implement An Adequate Audit Trail

* Dallas, TX; April, 1985: The failure to separately report numbers of ballots cast in each part of a split precinct produced ambiguous and suspect results.

* Elkhart County, IN; Nov., 1982: Changes in control cards, to compensate for errors that were discovered, were not documented; retest of the system, following the changes, was not done.

* Oklahoma County, OK; Nov., 1986: There were, in many precincts, significant differences between number of ballots tallied and number of voters reported as voting. In some cases the number of ballots tallied exceeded the number of reported voters. These differences made the results appear suspect.

4.13.3 Failure to Provide for a Partial Manual Recount

* Charleston, WV; Nov., 1980: The charges of conspiracy, and the expensive and time-consuming lawsuits, might have been avoided if the local laws had required, or allowed for, a partial manual recount without a court order. When the ballots were destroyed, the essential evidence to disprove an incorrect tally, of whatever cause, was made permanently unavailable.

* Dallas, TX; April, 1985: Although a recount was undertaken, it was a machine recount, using machines managed by the same organization. No manual recount, or recount managed by an independent organization, was done. Consequently, some suspicion remains.

* Moline, IL; April, 1985: A partial manual recount would have brought to light the incorrect results due to the ballot-reader failure, and would have prevented the losing candidate from being certified as the winner.

* Oklahoma County, OK; Nov., 1986: The unusual results in which lower-level contests received more votes than the contests on the top of the ballot could not be validated. Thus, a serious loss of public confidence could not be prevented.

* Palm Beach County, FL; Nov., 1984: The inability, under Florida law, for the defeated candidate to force a recount (because his race was insufficiently close), raised suspicions unnecessarily. A partial hand recount, as is done in California, might have prevented this situation from arising.

* A situation not appearing in this category, because an unofficial manual recount was taken in order to verify the different results obtained on an independently-managed system, is Carroll County, MD, November, 1984. The combined manual count and recount on an independently-managed system revealed the error in the original count.

4.13.4 Inadequate Ballots or Ballot Reader Operation

* Carroll County, MD; November, 1984: A recount, in which

read "checks" were ignored, showed slightly different tallies than the certified results. Chad is also believed to be responsible for some of the difference.

* Dallas, TX; April, 1985: The recount taken a few days after the election showed changes in ballots cast in 109 of the 250 precincts, and changes in votes cast for at least one of the candidates in 161 of those precincts.

* Gwinnett County, GA; Nov., 1986: The differences between results obtained on different computers reading the same ballots indicates the limitations of pre-scored punch cards in their ability to provide reproducible results.

* Moline, IL; April, 1985: Apparently, a slipping timing belt caused the reader to read incorrectly. The failure to provide for a partial manual recount (see above) or for sufficient pre-election testing (see above) prevented identification of the problem in a timely manner.

* Oklahoma County, OK; Nov., 1986: The ballot readers could not read up to 11% of ballots cast in some precincts.

* Palm Beach County, FL; Nov., 1984: The changes in votes cast on successive tallies of the same punch card ballots, probably due to the presence of chad, reduced the confidence of the losing candidate in the validity of the reported outcome.

* Stark County, OH; May, 1986: The final (third) count of ballots verified the first count, excepting that the results were slightly different due to chad fallout or deliberate removal of hanging chad by the inspection boards.

4.13.5 Inadequate Security and Management Control

* Elkhart, IN, Nov., 1982: Vote-tallying was done in a borrowed facility with equipment and employees not under management control. Multiprogrammed computer operations independent of vote-tallying and not under management control were being carried out while vote-tallying proceeded. A vendor representative was permitted to operate the vote-tallying process, and to change control cards without adequate documentation, and without regard to requirements for re-testing.

4.13.6 Inadequate Contingency Planning

* Oklahoma County, OK; Nov., 1986: No administrative rules were available to allow the counting of the significant number of ballots that could not be counted by machine. Many voters were disenfranchised.

* Salt Lake County, UT; Nov., 1980: No backup was available

when one of two computers failed during ballot counting. The result was a count much slower than expected.

4.13.7 Inadequate System Acceptance Procedures

* Oklahoma County, OK; Nov., 1986: The system procured was not adequately tested prior to acceptance. There was inadequate preparation to deal with the failures that later occurred.

5. APPLYING INTERNAL CONTROL TO COMPUTERIZED ELECTIONS

Many offices of election administration have not dealt with questions of accuracy, integrity, and security in a systematic manner. It appears that in many situations, responses to problems and concerns of this type have been on a case-by-case basis. Responses are even more fractionated when questions of accuracy, integrity, and security are treated separately.

The discipline of internal control, covering all of these factors from a mangagement point of view, has not been systematically applied to the operational aspects of election administration. This is not surprising, since election services are not priced for sale to its users, as are privately supplied services. Internal control has not been systematically applied in operational situations where transactions between an organization and its clients cannot be measured in money.

A proposed minimal extension in concept, described below in section 5.4.4, makes internal control applicable to election services. With this change, the systematic techniques of internal control may be used. Persons knowledgeable in the discipline may be employed or consulted to ensure the competent and coordinated application of appropriate techniques. The result should be the achievement of increased confidence in election outcomes.

5.1 Internal Control And Computer Security

In the past, internal control has been treated as a subject separate from computer security. An example of the earlier treatment is in Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management [81]. This 1974 publication (which remains pertinent at this time) has a separate section on internal control that is distinct from sections covering contingency planning and physical security. This treatment of internal control was adopted in the 1975 vote-tallying report, and in that report, also, a separate section on internal control was inserted to cover separation of duties and management of the program development process [82]. The distinction made in these reports is not surprising, in view of the disparate origins of the concepts of internal control and computer security. Internal control originated in accounting, while the source of computer security is computer science, itself an outgrowth of electrical engineering and mathematics.

A more recent treatment considers the two subjects in a more connected manner. A publication with a different understanding of the interconnected nature of the two subjects is entitled Work Priority Scheme for EDP Audit and Computer Security Review. As stated in this 1986 report:

> Security must be recognized as only one, albeit a major category of internal controls. ...computer security controls are a subset of the internal controls found in an automated information system. The major difference between these two sets of controls is that internal controls address efficiency and effectiveness in addition to security issues. [83]

Thus, in this study (and in much professional auditing literature), internal control is interpreted to encompass all controls, including computer security controls, used to ensure confidence in organizational systems. However, a need for distinctions between kinds of controls remains -- to facilitate their understanding and because various types of controls require specialized knowledge to assure their effective implementation.

5.2 Internal Control As Control Of Assets

Internal control is a management tool used within an organization. In the Federal Government, each department and agency is required to establish and maintain an adequate system of internal control under the Budgeting and Accounting Procedures Act (also called the Accounting and Auditing Act) of 1950. Requirements for applying internal control have been updated since 1950, with the Federal Managers' Financial Integrity Act of 1982.

One view of internal control is that it is for the purpose of controlling financial transactions and the use of tangible assets (primarily funds and property) in an organization. This concept of internal control is typified by the following definition, taken from the Federal Managers' Financial Integrity Act, and quoted in Circular No. A-123 (Revised) of the U.S. Office of Management and Budget (OMB):

> The plan of organization and methods and procedures adopted by management to provide reasonable assurance that:
>
> * obligations and costs are in compliance with applicable law;
>
> * funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and
>
> * revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets. [84]

For an office of election administration, internal control as defined above may be immediately applied to assure that computers owned by the organization are not stolen or misappropriated or, for example, to assure that the goods procured under purchase orders have actually been delivered. However, internal control as defined above is not applicable to non-financial operations such as vote-tallying, and this omission has created difficulties that need to be rectified. The public must have the same confidence in reported election results that it has in the reported status of its individual bank accounts.

5.3 Voting And Banking Operations: Accounting Similarities

The similarity of accounting problems in voting and in banking have been noted elsewhere. In the 1975 vote-tallying report, it was stated that:

> The problem of assuring correctness and security of vote-tallying programs is not significantly different than assuring correctness and security of computer programs used for sensitive financial and record-keeping purposes. Technical safeguards and management techniques developed for other applications can be adopted for vote-tallying programs. [85]

However, the similarity in control techniques is more widespread than just in computer programs. As noted by Ms. Suzan N. Kesim in the Texas legislative hearings (section 2.8.3):

> "Whether you are adding dollars or votes, you can apply many of the same auditing standards.... Many of the computer auditing procedures used by the banking industry that have been tried and true could easily be modified or used as they are for auditing elections.... "

In U.S. banking operations, the currency unit is the "dollar," while in another nation, the currency unit may be the "pound," "mark," "franc," "yen," or something else. The concepts of internal control will not change with a different hard currency unit, and they should not change if the currency unit is the "vote."

The voting process is very similar to a special kind of savings bank operation. Each candidate or issue alternative may be thought of as having an individual savings account, with the accounts grouped into contests. Each registered voter entering the polling place (or having an absentee ballot) may be thought of as a qualified depositor, having the right to make deposits to the contests for which the voter is entitled to vote. In a vote-for-one situation, the voter may deposit only one vote in one account per contest; in a vote-for-more-than-one situation, the voter may make deposits in more than one account per contest, but in almost all cases, may not deposit more than one vote per account.

If votes were treated as tangible assets and inherently valuable, like coins of denomination "one vote," they would be normally treated as subjects of internal control procedures. Then, accounting for the votes that the voters deposited could be carried out, and would be carried out as a matter of ordinary accounting practice. Each voter would have received the coins to be deposited at the assigned polling place, as part of the sign-in process. Each voter would have been previously approved as a depositor by virtue of having met certain qualifications such as those relating to age, citizenship, and residency.

Following the completion of the voting process, an internal auditor (a person who reviews the implementation and adequacy of internal controls) would be concerned with the assurance that none of the coins used were counterfeit, that persons receiving the coins to be cast as votes were truly qualified to receive them, and that the recorded account balances were correct according to the rules of the depositing process. To assure that account balances were correct, as well as to assure the return of the tangible assets, it would be necessary to account for the use and disposition of all coins, including those not voted for any candidate (undervotes), and those not voted according to the rules concerning number of votes per contest (overvotes).

Thus, one method of ensuring the applicability of internal control to vote-tallying is to treat votes as tangible assets. With this conception, controls may be applied to assure that only qualified voters are entitled to vote, and to assure that a full accounting is made of the disposition of all the votes distributed for use. With the use of internal control techniques in this manner, vote-tallying would be able to achieve the confidence of the public.

It may be noted that, in at least one way, voting is a more difficult process to audit than banking. In voting, the depositor (voter) is not given a record of his or her own account. Thus, the help that the depositors normally provide to the auditors in the verification of account statements cannot be present. Other verification techniques, such as manual recounting, must be used in vote-tallying to substitute for the inability of the voter to be of assistance for this purpose.

A more generic way of making internal control applicable to election administration, without the need to consider votes as tangible assets, is given immediately below. This change in concept would permit both voter registration and the voting process to be considered as subjects of internal control.

5.4 The GAO Concept Of Internal Control

With the passage of the Federal Managers' Financial Integrity Act of 1982, the U.S. General Accounting Office (GAO) was required, under the act, to develop and publish standards for the application of internal control in the Federal Government [86]. There is nothing in these standards that would restrict them to the Federal level, and with a broader definition of the term "transaction," they are applicable to any governmental function such as election administration. The GAO concept of internal control is used here, rather than other models, because it appears most appropriate for governmental operations.

In its publication, the GAO provided four purposes of internal control and a somewhat different definition of internal control than that given above. The GAO noted also that ultimate responsibility for good internal controls rests with management.

5.4.1 Purposes of Internal Control

The purposes of internal control identified by the GAO are as follows:

> * To help regulate and guide operations: Internal controls are not specialized systems within an agency. They should be recognized as an integral part of each system that management uses to regulate and guide its operations.
>
> * To achieve proper conduct with accountability: Internal controls are essential for achieving the proper conduct of Government business with full accountability for the resources made available.
>
> * To prevent undesired actions: Internal controls facilitate the achievement of management objectives by serving as checks and balances against undesired actions.
>
> * To achieve positive aims: Internal controls help achieve the positive aims of program managers.

It can be understood, from these purposes, that it is possible to view internal control from a broader perspective than just control of obligations and costs, and the safeguarding of assets. The purpose of achievement of positive aims provides an additional viewpoint for internal control: the effective execution of programs.

5.4.2 GAO Definition of Internal Control

The definition of internal control provided by the GAO is as follows:

> The plan of organization and methods and procedures adopted by management to ensure that:

* resource use is consistent with laws, regulations, and policies;

* resources are safeguarded against waste, loss, and misuse; and that

* reliable data are obtained, maintained, and fairly disclosed in reports.

The significant difference between this definition and the OMB definition provided in section 5.2 above is that the GAO definition is concerned with "resource use" whereas the OMB definition is concerned with "obligations and costs." Resources include personnel, and while some personnel may be part of a production process that converts tangible raw materials into tangible product, an important function of personnel in government is decisionmaking. Internal control must be concerned with decisionmaking, if it is concerned with the "proper conduct" of government business, the prevention of "undesired actions" and the achievement of "positive aims."

In election administration, some important decisions concern design and use of a voter registration system; procurement, acceptance, and deployment of vote-tallying equipment; scheduling of events to assure election readiness; ballot design; computer security; audit trails; the system for results dissemination and documentation; and the certification of winners.

Government operations often convert data into decisions, a process qualitatively different than manufacturing. In such a government operation, the real inputs and outputs have little economic relationship to the tangible materials (data storage media and computers) used. The data and decisions often have significant economic value and economic consequences, but these cannot be measured by the costs of the media and computers on which the data and decisions are recorded and processed. Thus, internal control, if it is to be maximally useful, cannot be based solely on safeguarding the tools of production. It must be concerned with the operational activity and the formation of the decisions that are the real products of the organization.

5.4.3 GAO General Standards

The internal control standards that the GAO specified are divided into two classes: general standards, and specific standards. The standards are intended to apply to all operations and administrative functions in an agency. In addition, the GAO specified that there should be prompt resolution of any finding or recommendation made by internal auditors that concerns an identified deficiency in internal control.

The general standards provide the foundation without which implementation of internal control would not be possible. The five general standards (identified below with the letter "G") can apply to any government agency, and are as follows:

> G1. Reasonable Assurance: Internal control systems are to provide reasonable assurance that the objectives of the systems will be accomplished.

This standard implies that the cost of internal control should not exceed the benefit derived. Thus, to determine a reasonable expenditure on internal control, an agency must identify the vulnerabilities inherent in operations, establish the level of risk (high, medium, or low) for each vulnerability, and determine the acceptable level of risk under varying circumstances. (Vulnerabilities of different vote-tallying systems were identified in chapter 3.)

> G2. Supportive Attitude: Managers and employees are to maintain and demonstrate a positive and supportive attitude toward internal controls at all times.

A positive and supportive attitude is ensured when internal controls are a consistently high management priority. General leadership is critical to maintaining a positive and supportive attitude toward internal control.

> G3. Competent Personnel: Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

Managers who possess a good understanding of internal controls are vital to effective control systems. Individuals should be given the necessary formal and on-the-job training.

> G4. Control Objectives: Internal control objectives are to be identified or developed for each agency activity and are to be logical, applicable, and reasonably complete.

Agency control systems may be classified into management, financial, programmatic, and administrative. Control objectives should be tailored to the specific responsibilities of each agency.

> G5. Control Techniques: Internal control techniques are to be effective and efficient in accomplishing their internal control objectives.

Internal control techniques are the mechanisms by which control objectives are achieved. Techniques include policies, procedures, plans of organization, and physical arrangements. To be effective, techniques should fulfill their intended purpose in actual application. To be efficient, techniques should be designed to derive maximum benefit with minimum effort. Efficient implementations make possible lower risks (see general standard G1) since a more efficient implementation implies a higher degree of control at the same or lower cost.

5.4.4 The Concept of a Non-Financial Transaction

In order to apply the GAO specific standards to the voting process, the traditional definition of "transaction" needs to be extended. According to the Handbook of EDP Auditing [87], transactions are:

> business events that can be measured in money and are entered in the accounting records.

In election administration, and in other services that are not priced for sale, the product of the organization is not measured in money. As pointed out above, it is decisions that define the process of election administration. Some of the decisions that personally concern the voter or the candidate include the following: registration of a voter, the removal of a voter's name from the registration file, the tender of a ballot (or the offer of the use of a DRE machine) to a voter at a polling location, and the certification of a contest result following the counting of the ballots.

These decisions concern the implementation of entitlements, specifically, entitlements to vote and to certification as a winner. The completion of the entitlement depends on satisfaction of certain necessary conditions. Some of the conditions may be voluntary, e.g., signing in at the polling place on election day, and others may be mandatory, e.g., receiving more votes than any opponent. Other non-priced operations (not necessarily in election administration) may be concerned with obligations, rather than with entitlements. Thus, a definition for a non-financial transaction is proposed as follows:

> an event, occurring in the course of organizational activity, that consists of a step in the implementation of an entitlement or an obligation and that is entered in the official records.

5.4.5. GAO Specific Standards

With this change in the concept of a transaction, the following six GAO specific standards for internal control (identified by the letter "S" to contrast with the general standard given above) are presented here for their application in election administration:

> S1. Documentation: Internal control systems and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.

According to the GAO, documentation of transactions or other significant events should be complete and accurate and should facilitate tracing the transaction or event and related information from before it occurs, while it is in process, and after it is completed. Here, support may be inferred for audit trails in vote-tallying, and for providing complete documentary support for a decision to certify the result of a contest.

> S2. Recording of Transactions and Events: Transactions and other significant events are to be promptly recorded and properly classified.

This standard extends the implementation requirements for standard S1 above. This standard applies to the entire process or life cycle of a transaction or event, including its authorization, initiation, processing, and final recording.

> S3. Execution of Transactions and Events: Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.

This standard provides support for assurance that only approved activities will be carried out. It provides a basis for the formalization of relationships between an election administration and its vendors, so that the activities carried out by a vendor during any election-related operation are fully authorized and controlled.

> S4. Separation of Duties: Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

To reduce risks, no one individual should control all key aspects of a transaction or event. Duties and responsibilities should be assigned systematically to a number of individuals to ensure that effective checks and balances exist. An example of this in election administration is the use of members of more than one party to serve jointly as election judges at precincts. Separation of responsibilities for computer program design and for computer operation is another example.

> S5. Supervision: Qualified and continuous supervision is to be provided to ensure that internal control ob-

jectives are achieved.

This standard requires that supervisors provide their staffs with the necessary guidance and training to help ensure that errors, waste, and wrongful acts are minimized and that specific management directives are achieved. To carry out this standard, expertise in internal control must be available in the organization. This need is considered further in section 5.6.

> S6. Access to and Accountability for Resources: Access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. Periodic comparison shall be made of the resources with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

This standard applies to tangible resources, for example, vote-tallying equipment, computer programs, and blank ballots. Blank ballots that have been printed for a specific election, in anticipation of the election, are similar to blank checks in their vulnerability. The GAO identifies blank checks as a type of resource which should be protected by being kept physically safe, having each separate document assigned a sequential number, and by assigning custodial accountability to responsible individuals. By analogy, blank ballots for a forthcoming election should be similarly treated. For computer programs, the working copies similarly should be kept physically safe, custodial accountability should be assigned, and the working copies should be compared with reference copies to assure complete agreement.

5.5 A Classification Of Internal Controls

A classification of internal controls is provided here in order to more specifically describe the application of the concept. In addition, certain specific recommendations of this report will be shown to be consistent with internal control techniques of a particular type.

Internal controls are divided into internal accounting controls and administrative controls. Internal accounting controls, which of primary interest, are divided into general controls and application controls. General controls concern the preparation of systems for the carrying out of operations, and may be called integrity controls. Application controls concern the actual processing of documents and data in the course of operations.

5.5.1 General Controls

These are the controls over computing and vote-tallying hardware, software, and facilities, but not the actual processing of votes

votes or of changes to the voter registration files. Hardware, software, and facilities concern both precinct locations and central locations. Specific categories of control include the following, where the titles in parentheses refer to similar categories identified and discussed in the Handbook of EDP Auditing [88]. Particular category definitions used here may be somewhat different, so that they apply more specifically to election preparations):

Access Controls (Data file security controls): These controls concern physical access to the computing and vote-tallying site or sites, electronic access through terminals and communications links, and access to separate data files, such as for voter registration. The controls are for the purpose of assuring that only authorized accesses are made, and only for authorized purposes.

Development and Implementation Controls (Implementation controls): These controls are for the purpose of assuring that the hardware and software of new systems, and authorized changes to existing systems, are correctly implemented and contain all necessary features (or meet certification/acceptance criteria in the case of procured hardware and software). These controls also concern assurance that all necessary preparations have been made for a computerized election, including specialization of software.

System Controls (System software controls): These controls are for the purpose of assuring that no unauthorized modifications are made to system hardware or software. System software consists of operating systems, compilers, and other computer programs not specific to any application. System hardware includes vote-tallying computers or devices of any type.

Application Software Controls (Program security controls): These controls are for the purpose of assuring that no unauthorized modifications are made to application software already in use.

Computer Operations Controls (Computer operations controls): These controls provide an audit trail for operation of the computing and vote-tallying devices, and concern the assurance of adequate backup and recovery procedures in case of malfunction.

5.5.2 Application Controls

These controls apply to the processing of documents and data in the course of the voter registration and vote-tallying processes. As above, titles in parentheses refer to similar categories identified and discussed in the Handbook of EDP Auditing [89]. As above, particular category definitions may be somewhat different, so that they apply more specifically to election operations):

Input Controls (Controls for completeness and accuracy of input): Completeness refers to the processing of each input document once and only once, while accuracy refers to the correct entry of the data on each document. In voting, completeness of input concerns controls over the voter sign-in process at precincts (e.g., to match number of voters against ballots issued), distribution and accounting for use of all ballots, the collection and transportation of voted ballots for processing, and the assurance that ballots are entered for counting once and only once. Accuracy of input in voting concerns the ability of the vote-tallying equipment to accurately read each ballot (or set of voter choices in a DRE system), and to accurately send and receive communicated precinct summaries. In registration, input controls are for the purpose of assuring the correctness of the entry of changes into the system that holds the list of registered voters.

Validity Controls (Validity controls): These controls help to prevent two types of problems: invalid input documents and invalid data on the documents. Controls to prevent counterfeit ballots may be considered to be in this category. In vote-tallying, these controls could help prevent a mixup in assigning ballots to an incorrect precinct during tallying. In registration, these controls could help identify voter addresses that do not exist, or are outside of a specified range.

Processing Controls (Controls for completeness and accuracy of update): In vote-tallying, these controls assist in the verification of the correctness of the results. If proper ballot accounting has been done (see Input Controls above), then reconciliation of votes cast with ballots cast can be accomplished, provided that records are kept on undervotes and overvotes. Recounting may be considered to be a control in this category. In registration, these controls provide assurance that the intended changes to the files have been carried out correctly. In registration, no arithmetic checks on summary data can be made, since the data is not being counted, like votes or money. However, the number of registered voters at the end of the day must be consistent with the number of registered voters at the beginning of the day, given a particular number of registered voters added and deleted.

File Maintenance Controls (Control techniques employed for maintenance): This type of control helps assure currency of data in the registration file, and supporting geographic, geocoding, and postal information files. It does not apply to vote-tallying.

5.6 The Discipline Of Internal Control

5.6.1 Link to a Professional Body of Knowledge

Internal control is a professional body of knowledge that is known, taught, and applied by internal auditors and EDP (electronic data processing) auditors. Professional associations that are concerned with the subject of internal control include the

American Institute of Certified Public Accountants, 1211 Avenue of the Americas, New York, NY 10036, (phone: 212-575-6700);

Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, (phone: 407-830-7600); and the

EDP Auditors Association, 455 Kehoe Boulevard, Carol Stream, IL 60188 (phone: 312-682-1200).

Since internal control is part of a professional body of knowledge, the concepts and application of internal control can be learned in an organized, consistent, and uniform manner by elections personnel. Publications, both professional journals and textbooks, are widely available. Professional conferences are held annually or more often.

5.6.2 Job Functions for Internal Control

The need for implementation of internal control concepts could be satisfied by the establishment of appropriate job functions in the office of election administration. Examples of appropriate job functions are given in Guide to Auditing for Controls and Security: A System Development Life Cycle Approach [90], a publication of the National Bureau of Standards. This publication identifies separate "internal control officer" and "system security officer" positions. The publication envisions that, in a large government department, there would be senior officer positions at the department level, and separate "specialist" positions at the operational level, but this concept may not be applicable to an office of election administration in a local government. In local government, it may be advisable, due to budgetary and workload constraints, to fold in the "system security officer" responsibilities into the "internal control officer" position. A person in data processing, knowledgeable in computer security, could be trained in the additional techniques of internal control to occupy this position.

The responsibilities of the "internal control officer" might be specified as follows:

> The internal control officer (ICO) establishes internal control (including computer security) policies and ensures that operational systems comply with these policies. The ICO assures that each operational system meets basic standards for documentation, recording of transactions, execution of transactions, separation of duties, access to resources, and all other internal control requirements.

In addition to the ICO, the employment of an internal auditor could be considered. Typically, the internal auditor reports to the senior management official, or to the board of directors. The function of the internal auditor is to independently review the implementation of controls and provide reasonable assurance to senior management that the organization is functioning adequately with regard to legal requirements, management policies, internal controls, audit trails, documentation, and economy and efficiency.

If the election administration cannot fund these positions full time, then discussions could be held with other agencies of the same local government to consider the possibility of jointly funding the positions. The local government could consider itself equivalent to the department for which a complement of positions are envisioned in the reference [90] identified above.

State-level support for these positions is another possibility. Joint funding or State-level support might engender a wide review of computer security policy and implementation activity, a worthwhile activity in any event.

6. DETAILED CONCLUSIONS AND RECOMMENDATIONS

The conclusions and recommendations presented in this chapter cover three general areas: institutional concerns; hardware and software performance, design, and integrity; and operational procedures. Institutional concerns are considered in sections 6.1 through 6.6. Hardware and software are covered in sections 6.7 through 6.12. Operational procedures are discussed in sections 6.13 through 6.17. In the final section, 6.18, the recommendations are shown to be responsive to specific problems of computerized vote-tallying identified in section 2.9.

INSTITUTIONAL CONCERNS

6.1 The Continuing Problem Of Confidence In Results

Consultants' evaluations of a vote-tallying program, quoted in the New York Times article on July 29, 1985 [6], as well as testimony on November 25, 1986 before a committee of the Texas legislature (section 2.8.3 above), have demonstrated that technically trained individuals continue to find significant vulnerabilities in vote-tallying software and hardware. Results of computerized elections continue to be challenged, and regardless of the outcomes of these challenges, it has been clearly shown that audit trails that document election results, as well as general practices to assure accuracy, integrity, and security, can be considerably improved.

Technically qualified consultants employed in some election challenges have stated that "it would be possible" to alter computer programs used in those situations. While proof of actual manipulation appears to be lacking, documentation conclusively demonstrating otherwise is insufficient, due to the manner in which the challenged elections, and others, have been conducted.

In the 1975 vote-tallying report, it was stated that:

> The assurance that steps are being taken by election officials to prevent unauthorized computer program alteration or other computer-related manipulations remains, nationwide, a problem for the maintenance of public confidence in the election process. [91]

Thus, the 1975 statement remains pertinent.

Given the continuing problem, it is important, first, to identify the agencies responsible for correcting the deficiencies, and second, to provide recommendations that will assist these agencies in rectifying the situation.

6.2 Responsibility And Requirements For The Effective Management Of Elections

6.2.1 Government Responsibility

As discussed in section 3.9.1, responsibility for the conduct of elections in the United States rests with local governmental agencies assigned this function under State law (or under local law, under a grant of authority by State law). It was stated in that section that major elections are carried out by about 2870 county-level government agencies, and by some 7630 other local governmental agencies. In some 1005 of the total 3140 counties and county-equivalents, vote-tallying is completely computerized. It is partly computerized in an additional 192 counties.

Typically, the local offices operate with oversight by the chief State elections official, but the degree of oversight varies from State to State. The local offices of election administration require the necessary resources and expertise to efficiently and effectively carry out their responsibility. That responsibility includes procurement of supporting equipment and services, including vote-tallying systems. An effective procurement must include specifications (technical descriptions of products to be procured) so that accuracy, integrity, and security will be promoted.

6.2.2 Expertise and Effective Management

In the 1975 vote-tallying report, it was noted that:

> There is a lack of expertise in computer technology available within the structure of many local election administrations. In jurisdictions without technological expertise, vendors are more likely to conduct a significant part of the election on the administration's behalf. [92]

To some extent, this lack of expertise continues to exist, particularly in the smaller jurisdictions. The example of Elkhart County, Indiana, described in section 4.4.1, is a glaring instance of the problem.

There is no dispute over vendor involvement in vote-tallying. As was testified in the Texas legislative hearings by an executive of a major election equipment vendor (section 2.8.3):

> "People are going to have the best elections that well-intentioned honest people can run, and that well-intentioned honest companies can run...."

Vendor involvement may be excessive when there is a lack of local competence. However, vendor goals are not identical to those of the responsible public officials. Excessive involvement by a vendor, i.e., the assumption of management prerogatives, may be in violation of GAO standards for internal control. Pertinent GAO standards are G3 (section 5.4.3), and S3 and S5 (section 5.4.5). These are:

> G3. Competent Personnel: Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.
>
> S3. Execution of Transactions and Events: Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.
>
> S5. Supervision: Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

In the 1975 vote-tallying report, it was concluded that:

> Each State should insure that each of its local jurisdictions possesses the necessary expertise in computer technology to carry out its statutory election functions and does not rely primarily on vendors of election system components. [93]

This recommendation remains pertinent, and now is buttressed with internal control standards.

Difficulties with vendor-supplied products used in vote-tallying are often indicators of a lack of expertise and/or lack of adequate management control in the affected agency. In one of the New York Times articles on computerized vote-tallying, it was reported that a leading computer security expert had stated that:

> "the degree of fraud controls built into a program is largely determined by the end user." [9]

It is the responsibility of the State and local election administrators (the end users) to ensure that requirements for adequate audit trails and other fraud-prevention techniques are included in the specifications to be met by acceptable computerized vote-tallying systems.

Failures in organizational use of technology often indicate failures in management. In the Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident [94], it was recognized that the immediate cause of the accident was a failure of a joint of a rocket. However, deficiencies in management were cited as causes of the failure to correct the design defect. The Commission reported that neither the contractor nor the government agency "responded adequately to internal warnings about the faulty seal design," that "a redefinition of the Program Manager's responsibility is essential," and that a new office having "direct authority for safety, reliability, and quality assurance" should be established.

It remains true, as stated in the 1975 vote-tallying report, that:

> Technology and the management of technology are inextricably linked. The effective use of technology requires management control; and the effective management of technology requires the utilization of appropriate technological expertise. [95]

6.2.3 Requirements

If each office of election administration is to effectively carry out its responsibilities, it must have in place the necessary technological expertise and management control systems. These supporting elements are most urgently needed in the following three areas: (1) procurement of vote-tallying hardware and software, (2) preparation of vote-tallying systems for elections, and (3) execution of vote-tallying operations. To the extent that local administrations cannot acquire the necessary knowledge and personnel, the State-level activity should provide it.

6.2.4 FEC Clearinghouse Performance Specifications

With regard to procurements, the 1975 vote-tallying report specifically recommended statewide specifications [96]. The FEC Clearinghouse performance specifications [2] [3] are approaching completion (see section 2.4), and they are intended for statewide adoption. Each State should consider the adoption of these specifications when they are issued.

6.3 Implementation Of An Internal Control Function

Concepts of internal control (as extended to non-priced operations, described in chapter 5), should be utilized by election administrators to help assure accuracy, integrity, and security in elections. Procedures adopted for these purposes should be consistent with and supportive of the GAO internal control standards presented in sections 5.4.3. and 5.4.5. Many of the recommendations made in 1975 could have been classified as internal controls, under a newer interpretation of the subject.

Internal control expertise should be added to the personnel complement in election administration to assure understanding and implementation of the concepts. Internal control is a professional activity; training in the discipline, texts, and a community of practitioners are available. In a small election administration, the internal control function could be added to the duties of the individual responsible for implementation of computer security controls, provided that additional training is given.

Additional confidence in the reported results of elections could obtained if an internal auditor was available to independently review the implementation of internal controls and report on their effectiveness.

Internal control personnel could be shared with other agencies of the same government, or provided by the State, if the election administration has insufficient resources to offer full-time employment.

6.3.1 Outside Recommendations vs. In-house Expertise

Specific procedural recommendations to help assure accuracy, integrity, and security were provided in the 1975 vote tallying report, and similar recommendations are provided below. However, the failure of a significant number of election administrations to implement the 1975 recommendations is indicative of the need for a different kind of answer.

There is an essential qualitative difference between the availability of recommendations made in an outside consultant's report and the availability of in-house professional expertise familiar with the necessary body of knowledge. Expertise within the organization provides the capability to deal with questions of accuracy, integrity, and security on a day-to-day basis, to evaluate outside recommendations for feasibility and cost, and to implement realistic solutions based on local conditions and the immediate situation.

6.3.2 Achievement of Management Goals

The involvement of an internal controls officer in the implementation of a voting system, and the involvement of an internal auditor in the review of such a system, will provide an elections administrator with additional capability to pursue established goals. The involvement of internal control personnel should relieve the elections administrator from having to be personally knowledgeable about specific technical matters best left to individuals who are professionally qualified in that field. With the necessary technical expertise on staff, an elections administrator can retain responsibility for direction, and can perform the required supervisory role to assure that established goals, such as accuracy, integrity, and security, will be achieved.

6.3.3 Analysis of Risks and Impact on Public Confidence

An important function of internal control is to organize the identified system vulnerabilities into a set of realistic threats and responses. This activity requires the performance of a risk analysis [81]. The analysis involves a determination of the likelihood of actual exploitation of a particular vulnerability, identification of the potential loss or negative impact from the executed threat, and development of proposed countermeasures that include associated costs. A risk analysis would consider, for example, the possibility that "computers can be manipulated remotely, by wire or radio" or that "the software can be set to await the receipt of a special card, whose presence will cause all the election counters to be altered" (threats specifically identified in public testimony).

The result of a risk analysis and its follow-on activities would satisfy two needs. These needs are, first, for actual system protection plans, and second, for assurances that could made to the public that the potential threats are understood, have been prioritized for significance, and are being countered with available measures consistent with resources.

Internal control personnel would be extremely valuable in responding to questions about accuracy, integrity, and security raised by supporters of defeated candidates or by technically trained members of the general public. The involvement of professionally qualified internal control personnel should provide the general public with additional confidence that a computerized election with which these personnel have been connected has been carried out fairly and accurately.

6.4 Review Of The Adequacy Of State Laws And Regulations

Each State should examine the adequacy of its laws and regulations to assure their effectiveness in treating problems of accuracy, integrity, and security in computerized vote-tallying.

6.4.1 Revised Texas Statute on Electronic Voting Systems

At a minimum, the requirements of the revised Texas statute on electronic voting systems should be considered for adoption in those States that have not already adopted equivalent provisions. Provisions of the Texas statute include requirements for audit trails, deposit of computer programs with the secretary of state, assurance that the programs used in vote-tallying are identical to those deposited, mandatory one percent manual recount of all contests, testing of equipment using all applicable ballot formats, disconnect of remote terminals during vote tabulation, and specific scrutiny of ballot count discrepancies when they occur at precinct locations (see section 2.8.4).

6.4.2 Effective Use of Technical Terminology

In connection with the examination of laws and regulations, a review should be undertaken of the technical terminology employed. The latter review should assure that the use of such terminology is clear, and is consistent with current concepts.

6.5 Future Vote-Tallying Systems

While vote-tallying using on-line systems (e.g., through telephones or stations similar to automatic teller machines) is technologically feasible, the decision to implement such systems must be based on more fundamental factors. The principal issues should be political and social concerns, as well as concerns for the benefits compared with the costs.

Any installed system must meet several basic political requirements, in addition to technical requirements of accuracy and reliability. The political requirements include equal access by individuals to the voting franchise, the ability to verify registration, the ability of voters to vote in secret without intimidation, assurance of fairness to opposing parties, and the ability to demonstrate, through audit trails and other internal controls, that the announced results are correct. The benefits of the use of the advanced technology might be greater convenience to voters and possibly greater participation. However, the costs of providing the capacity for very high traffic over a short time span might be prohibitive.

6.6 Transfer Of Technical Knowledge To Election Officials

Technical knowledge that can be collected and made available on a national basis needs to be transferred to election officials. The activity of information dissemination being carried out by the Election Center (see section 2.5) should be expanded. Election officials need sources of knowledge in new and improved techniques of management, including those that would assist in the solution of problems of procurement and operations. The need for sources of technical knowledge has been previously recognized:

> "State election officials agree generally on the need to upgrade election procedures by providing more technical guidance to local officials, particularly in such areas as the utilization of electronic data processing techniques." [97]

HARDWARE AND SOFTWARE PERFORMANCE, DESIGN, AND INTEGRITY

6.7 Adoption Of FEC Clearinghouse Concepts For Product Acceptance

Acceptance procedures for hardware and software should be consistent with the FEC Clearinghouse implementation plan [4] involving qualification and certification prior to final acceptance. Qualification implies conformance with standards and functional requirements. It may be done for a vendor by an independent testing laboratory in order to satisfy the requirements of many States with a single set of tests. Certification is a State approval process; it ensures that the product meets State requirements. Acceptance testing is performed at the local government level; it evaluates the degree to which the specific units delivered conform to the characteristics of the product that were approved under qualification and certification.

6.8 Software Certification, Performance, And Integrity

6.8.1 Certification of Software

Products to be certified should include all software that is to be used in connection with vote-tallying. This software includes operating systems, compilers, and other utility programs that run with application programs. Application programs include software for specializing vote-tallying programs for a particular election, and the vote-tallying programs themselves. The software should include system programs that compile source application programs to object code. If an election management package is to run on a computer at the same time as specialization or vote-tallying software, that package should be certified at the same time.

6.8.2 Requirements for Certification

Requirements for certification should include one type of assurance for all software and a second type only for vote-tallying software. All software should be checked for integrity, that is, for the ability to carry out its asserted function and to contain no hidden code. Vote-tallying software should be tested, in addition, for logical correctness. Software testing may be part of a qualification process, done once, that is acceptable to many States.

6.8.3 Integrity of Software

Separate copies of all computer software, such as the operating system, compiler, and other needed utility programs, as well as vote-tallying software, should be obtained from general suppliers from a stock of publicly offered products, or should be written in-house. With each procured software product, complete documentation of its functions should be obtained. Assurances should be received from each supplier that the copies obtained perform no other function than that stated in documentation of the products.

Assurances may be simple written statements, or detailed statements specifying the function of each major program segment. In addition, tests may be performed to demonstrate the correctness of the assertions.

For support software, such as operating systems, available resources may limit the tests that can be performed to assure integrity. Qualification, done once to satisfy many States, may enable testing resources to stretch further. If available resources severely restrict integrity testing, written statements by the manufacturer and documentation of functions may be all the assurance that can be achieved. Thus, reliability and accountability of the sources are essential. Copying of software from unaccountable sources must be forbidden.

6.8.4 Dedicated Operation and Use

An important procedure to assure system integrity is to isolate vote-tallying and support software from influences over which the election administration has no control.

Any routine (even a simple routine used to copy files) that operates on any vote-tallying program should be maintained separately under the control of the election administration and not used for any other purpose except in connection with vote-tallying.

When vote-tallying software is run on a general-purpose computer in which there is no control over the other applications or support software that are also being run, a review for hidden code is not useful. Hidden code may be present in other software that is not reviewed, and may be transferred to the vote-tallying software as a "computer virus." Thus, it is strongly recommended that vote-tallying software not be allowed to run on a multiprogrammed general-purpose computer. The restriction to dedicated operation and use were recommended in the 1975 vote-tallying report. [98]

For vote-tallying with DRE machines, running of any software related to vote-tallying together with other software that has not been reviewed for hidden code should be prohibited. With DRE systems, freedom from hidden code of all software associated in any way with vote-tallying must be guaranteed. There are no ballots that can be recounted as a check on system correctness.

6.8.5 Logical Correctness of Vote-Tallying Software

For vote-tallying software (including software for election specialization and ballot generation, as well as vote-summarizing software), certification implies assurance of logical correctness: for example, in implementation of ballot position assignments in ballot generation, in translation of voters' choices to storage, in summation of voters' choices regardless of rotation, and in implementation of State logical rules such as for overvoting and crossover voting. No requirement for certification of logical correctness is implied for other types of software.

6.8.6 Design for Specialization and Prevention of Logic Changes

After software has been certified, no changes should be permitted without a re-certification. Vote-tallying software should be designed so as to require that specialization occur only by a "fill-in-the-blanks" process in tables. This concept was presented in the 1975 vote-tallying report under "Use of Table-Driven Programs." [99]

It should be noted that the use of "header cards" in vote-tallying operations constitutes part of the specialization process. Data provided to the program by header cards should only fill in blanks in tables and should not change program logic. As noted in the 1975 vote-tallying report, a complete audit trail of operations would have to include "capability to copy out on the output printer the exact contents of each header and other control card read at the input..." [100]

6.8.7 Deposit and Availability of Certified Software

All software that has been certified should be deposited with the chief election official of the State. The materials on file should not be public information, but should be made available to law enforcement authorities, on proper application, for investigation of election irregularities.

6.9 Accuracy Of Ballot Reading

The problems found in ballot reader inaccuracy, both in the count of ballots, and in the count of votes on the ballots, are a significant source of lack of confidence in vote-tallying by candidates and informed observers. The use of pre-scored punch card ballots contributes to the inaccuracy and to the lack of confidence. In every case reported in chapter 4 in which a recount was taken using pre-scored punch card ballots, the second vote count differed somewhat. It is generally not possible to exactly duplicate a count obtained on pre-scored cards, given the inherent physical characteristics of punch card ballots and the variability in the ballot punching performance of real voters.

The statements made in the 1975 vote-tallying report about the need for ballot reader accuracy included the following:

> The sensor [i.e., ballot reader], the device which converts information on a ballot to electronic form for data processing, is one of the key elements of a computer-based vote-tallying system. Its accuracy, reliability, and stability over time must be assured. .... Sensor accuracy must be considered in combination with the quality of its data input which the voters are able

> to achieve given particular forms of ballots and vote-encoding equipment. ... The effect of a sensor on the information contained on a ballot must be minimal when the ballot is read. This is extremely important if a ballot must be re-read or recounted. [101]

These statements continue to be pertinent.

Therefore, the following recommendations are made:

6.9.1 Accuracy Goal

A recommended goal for computerized vote counting is that the vote count produced on a computerized ballot-tallying system should be able to be reproduced on a recount with no more than a change in one vote for each candidate or issue alternative in ballot quantities of up to 100,000 when machine-generated (ideal) ballots are used. The ballot reader should be able to tolerate a wide range of voter punching/marking behavior without a significant increase in error.

6.9.2 Elimination of Pre-scored Punch Card Ballots

The use of pre-scored punch card ballots should be ended.

One method now available to eliminate pre-scored cards, while retaining the "votomatic" concept, is with a new type of stylus. This stylus permits a voter to create a hole of consistent dimensions in a ballot card without the need for pre-scoring. A replacement for the internal construction of the "votomatic" ballot holding device must be installed in conjunction with the use of the new type of stylus. Other devices and methods for elimination of pre-scored punch card ballots also may be effective.

6.9.3 Treatment of Rejected Ballots

Some ballot readers (primarily mark-sense readers) include a "go-no-go" decision, depending on whether the reader can read the ballot at all. Such readers may refuse to count ballots in the "no-go" status. Administrative regulations should require such rejected ballots to be counted manually, so that no voter loses the voting franchise because of machine failure.

The use of the term "rejected ballots," implies that none of the ballot readers used could distinguish a hole from no-hole or mark from no-mark at a location on a ballot at which a hole or mark indicates an intention to cast a vote. If a ballot reader can correctly distinguish the voting intentions made by the voter in all the appropriate locations on the ballot, it is successfully reading the ballot (even if a voting intention cannot be counted because of an overvote or the voter submitted an undervote by failing to vote for an office). If the ballot is correctly read, the term "rejected ballots" should not be used.

6.9.4 Required Research

Research to determine the accuracy of current ballot reading systems (such as that now being carried out by ECRI of Plymouth Meeting, PA), and additional research to improve ballot tallying systems from the standpoints of both accuracy and ease of voter use, are important to pursue. The need for such research was recognized in 1975. [102]

6.10 Design Of DRE Machines

As no voter-generated records of voters' choices exist with the use of DRE machines, and no recount of voters' choices is possible, additional steps should be taken with these machines to assure confidence in the reported results.

6.10.1 Recording of Each Undervote

It is recommended, therefore, that each DRE machine be designed so as to take a positive action for every contest in which the voter fails to vote the maximum number of times permitted. The positive action should be the recording of a "no vote" for each undervote. In a vote-for-two contest, for example, if the voter only votes for one candidate, the machine should cast one "no vote." In a vote-for-two contest, if the voter fails to vote at all, the machine should cast two "no votes." The machine should be designed to take this action only when the voter indicates to the machine that voting choices are complete.

The "no vote" should be recorded for each separate contest, so that if a voter-choice set is retained, the presence of each "no vote" should be clearly present as a separate indication. That is, the "no votes" should not be computed in summary form as the difference of the maximum number of votes possible less the actual number of votes cast. (If there is an actual "none of the above" possibility for voter consideration, as is the case in at least one State, the voter still may fail to select it or otherwise make any candidate selection.)

The implementation of the positive "no vote" indicator may be better explained if the DRE function of precisely recording the voter's choices is considered to consist of two substeps. The first of these substeps consists of the setting of indicators seen by the voter in response to the voter's particular selections. If the machine is initially set up for voter use so that each contest has a number of "no vote" indicators equal to the maximum number of allowable votes in the contest, the voter's actions can be logically treated as replacing each "no vote" indicator, one at a time, with an actual candidate or issue alternative selection. (The "no vote" indicators need not be seen by the voter.) If the voter fails to vote the maximum times allowed for the ballot configuration, some "no vote" indicators will remain when the voter indicates to the machine that voting is complete.

The second substep occurs immediately after the voter indicates that voting is complete; it consists of the transfer of the set of selections to a more permanent storage. At that time, the remaining "no vote" indicators that were not replaced would be transferred to permanent storage with the actual candidate and issue alternative selections. The sum of the number of actual votes and "no votes" transferred would have to be the same quantity for every voter using the same ballot style. The presence of this constant quantity for each voter would provide support for the supposition that the second substep operated correctly, i.e., that the indicators resulting from the first substep, including both actual voters' choices and unreplaced "no votes," were actually transferred to permanent storage.

The design of a DRE machine in this manner will provide additional confidence that, when an undervote is seen in the results, the undervote is actually due to the voter's choice not to vote, instead of the machine's failure to record the voter's choice. The design will provide a distinct improvement over the situation with a lever machine. In the use of a lever machine, it is not possible, without an examination of the internal operation of the mechanism, to distinguish a voter's failure to vote from the machine's failure to record a vote.

The constant value of the sum of the number of unreplaced "no votes" and the number of votes for candidates and issue alternatives, provides the capability of an arithmetic cross-check on the action of the machine (see section 6.17.3).

6.10.2 Retention of Voter-Choice Sets

Each voter-choice set (i.e., the machine's record of all choices of a voter) should be retained in the machine on a removable, non-volatile medium, for example, magnetic disk. Storage locations of the voter-choice sets would have to be randomized to prevent association of a particular set of choices with a particular voter. The retention of the voter-choice sets makes possible a verification, on an independent machine, of the DRE machine's summation of its recorded voters' choices (see section 6.17.4). This verification only checks the summation process; it does not check the data entry process. By design, there can be no independent verification of the data entry process. The latter can be checked only by testing the machine's response to known inputs (see section 6.17.5).

6.10.3 Accuracy of DRE Machines

Analogously with ballot-tallying machines, an accuracy goal can be established for DRE machines. For a statistical test of accuracy, a device simulating a large number of voter selections could be used. The test would verify that a selection of any ballot position translates to a correct machine-produced result.

A goal analogous to that stated for ballot-tallying machines is that for known selections made in up to 100,000 ballots cast, there should be a discrepancy of no more than one vote in the results provided for any ballot position.

6.11 Certification Of DRE Hardware Logic

As there are no independent ballots that can be recounted in a DRE system, it is essential to assure that DRE hardware logic, as well as its software, is correct. DRE hardware should be certified for logical correctness, by examination of the logic design and by testing under a large variety of different conditions. A typical unit and its documentation should be deposited with the State, under the conditions specified in section 6.8.7.

6.12 Selection Of A Vote-Tallying System

The discussion of chapter 3 above has demonstrated that every type of vote-tallying system has its vulnerabilities. Every type of vote-tallying system has relative advantages and disadvantages.

It is possible to effectively utilize any of the computerized systems discussed in chapter 3 provided that:

(a) procurement specifications are well-written in accordance with required performance, including considerations of accuracy, reliability, and recommended design concepts;
(b) certification and acceptance tests are designed so that only an acceptably performing system is acquired;
(c) the vote-tallying system (including personnel and back-up) is adequately prepared, tested, and put in readiness;
(d) standard procedures and recommended internal controls (including audit trails and integrity controls) are in place for voting and vote-tallying operations; and
(e) administrative regulations have been designed and are in place to deal with expected activities, as well as with any contingencies that might arise.

OPERATIONAL PROCEDURES

6.13 Pre-Election Checkout

Lack of sufficient pre-election testing appears to be a major source of current operational difficulty. The Illinois State Board of Elections, based on their investigations, called for "extensive" pre-election testing, and reported that "the testing of computer vote tabulation systems needs to be improved substantially" (see section 4.6). This recommendation should be heeded by election administrators. As was pointed out, similarly, in the 1975 vote-tallying report:

> To the greatest extent possible, all hardware and software to be utilized should be given a dry run simulating specific conditions to be faced on election day and election night. [103]

Sufficient pre-election testing should be applied so that errors in software specialization or in implementation of logical rules, if any, will become obvious. A large variety of possible voting combinations should be tested. A dry run involving key personnel is valuable, particularly in the first use of a new system.

Adoption of the testing clause from the revised Texas statute on electronic voting systems (see section 2.6.4) is recommended as a minimum standard. The statute states that "each unit of automatic tabulation equipment shall be tested, using all applicable ballot formats..."

6.14 Implementation Of Audit Trails

Two types of audit trails must be distinguished. One type records steps in the operation of computing equipment (both the operation of central equipment by computer operators and the operation of precinct-located equipment by precinct officials). The second type records steps in the execution of the voting process and includes all steps from the printing and distribution of blank ballots, through collection and processing of voted ballots, to the summarization of precinct results.

Principles of internal control require that both types of audit trails be maintained. The following statement in the revised Texas statute on electronic voting systems is strongly supported:

> "A voting system may not be used in an election unless the system ... is capable of providing records from which the operation of the voting system may be audited."

Audit trails provide much of the documentation through which the correctness of the reported results may be verified.

6.14.1 Full Ballots-Cast Data from Split Precincts

A "split precinct" is a precinct in which more than one ballot style is used. As certain contests might appear on some ballot styles but not on others, it is important to report ballots-cast data and corresponding voter participation data for each split. A complete audit trail for each contest is obtained only with the reporting of such data. Complete reporting may be simply accomplished by designating each split a separate precinct, or special arrangements may be made to report split data from a single precinct. It may simplify the voter sign-in process and the reporting of voter participation if there are separate precincts. The precincts may continue to be located at the same polling place.

6.15 Access Controls

6.15.1 Site Controls

Controls must be in place to restrict access of persons to sites or parts of sites where computing equipment, blank ballots, voted ballots, and signature lists are located. This includes locations at precincts where computers, DRE machines, and election supplies are stored in preparation for use.

6.15.2 Equipment Access Controls

Controls should further restrict access to equipment (both central and precinct-located) for operation or maintenance to designated individuals. Controls on access to equipment should prevent removal or tampering with portable components, e.g., plug-in read-only memories, removable magnetic tapes or disks, plug-in circuit boards, etc.

6.15.3 Transportation and Handling Controls

Access to the transportation and handling of signature lists, blank ballots, voted ballots, and removable read-only memories containing programs and election data, must be controlled.

6.15.4 Voting Process Controls

At locations where voting takes place, controls should assure an orderly flow of voters, not only to assist voters to quickly and efficiently complete the process, but for security purposes. Controls should assure that no voter or other person can tamper with, replace, or deface a "votomatic" ballot insert, "datavote" ballot punch, or DRE ballot display, or carry away a mark-sense marking pencil, "votomatic" stylus, information display, or any other equipment or supplies needed for voting. In ballot-tallying systems, controls should assure that only registered voters receive ballots, and that each voter receives only one ballot and votes the ballot given. In DRE systems, equivalently, controls should assure that only registered voters have access to the machines, and that each voter votes only once.

6.15.5 Telecommunications Security Controls

If voting data are transmitted from a remote to a central location, controls must be in place to assure the security of the process. The "dial-out only" procedure, in which the central location dials out and verbal communication establishes, through name and password, that the person at the remote location is the responsible individual, is satisfactory for establishing the connection from the central location to the remote location. More complex controls have been given in a previously cited reference [31]. If results are to be transmitted before the polls are closed, or if individual votes are to be transmitted, or if the data transmitted is to be considered official, then controls to secure the content of the message must be employed. The computer data authentication process previously referenced [34] should be used.

While concern for the security of transmission is included in this section as an access control, assurance of the accuracy of transmission is considered to be an application internal control.

6.16 Application Internal Controls For Ballot-Tallying Systems

The controls in this section are similar to those proposed in the 1975 vote-tallying report under the headings of aids to audit of calculations, effective control of ballots and computer hard-copy records, and use of teleprocessing [104].

6.16.1 Controls over Blank Ballots Printed and Distributed

A significant problem in ballot-tallying systems is the protection of the system against all types of ballot frauds. Controls must be instituted over the number of blank ballots printed and the number of blank ballots distributed to each polling location. Documentary evidence of these activities should be retained.

6.16.2 Numbering of Ballot Stubs

One way of assuring better control over ballot distribution is to have the ballot stubs numbered and assembled in groups (e.g., fifty or one hundred). The assignments of ballot groups to each polling location should be recorded. The individual ballot stub number may be recorded by a precinct official when a ballot is issued to a voter. The stub number is used to assure that the ballot to be voted is the same one issued.

6.16.3 Controls over Ballot Use

The number of voted ballots (of each individual type, in case each voter is issued more than one type), must equal the number of voters that were issued ballots (i.e., signed in to vote). At each precinct, the number of blank ballots initially received must be equal to the sum of the ballots returned in all categories (e.g., voted, voted but challenged, spoiled, and unused). When the ballots from all precincts are returned to the administrative center, the total number of all ballots returned in all categories (plus the number unreturned by absentees) should equal the total number of all ballots distributed to all precincts and to absentees.

6.16.4 Control of Ballot Validity

Ballots may be watermarked or otherwise made distinctive to guard against counterfeiting. Procedures used by the manufacturer and vendor of the ballots should be reviewed for security.

6.16.5 Machine-readability of Ballot's Precinct Number

Machine-readability of the precinct number assists in the prevention of ballots from one precinct being mixed with or exchanged with ballots of another precinct. The computer counting the votes must be programmed to read the precinct number and make effective use of it, if the machine-readable identification is to have any value.

This check is extremely important if "votomatic" cards are used, particularly if ballot rotation (i.e., different candidate sequencing in different precincts) is employed, or if counting of ballots of more than one ballot style is done at the same physical location. If equal numbers of "votomatic" ballots (ballots having no candidate information on them) were exchanged between precincts using different rotations, and a check of precinct numbers were not done, the mistake would not be discovered by a ballot count reconciliation. The correct number of ballots would be found for each precinct.

The programmed check of the ballot's precinct number also reduces the importance of correct computer operator action in processing the ballots. With a computerized check of precinct number, it is not necessary for the operator to insert a "header card" with this information on it, provided that the ballot style for the precinct is already recorded in the computer. If ballot style were used as the machine-readable value, the use of a "header card" would still be necessary to enable a precinct-by-precinct count, if more than one precinct employed the same ballot style. The possibility of operator error in using an incorrect "header card" is eliminated only with use of the machine-readable precinct number.

6.16.6 Accuracy of Telecommunication of Voting Data

Telecommunication of summarized precinct tallies is being used in many jurisdictions to speed up processing of unofficial results on election night. For this application, slower speed and lower cost asynchronous transmission may be used. Accuracy protection using parity checks with retransmission in case of error is satisfactory for this application. This form of protection is available with many modems.

If data is to be transmitted before the polls close, or if the transmitted data is to be a part of official, final results, then more protection is necessary. In these cases, the standard on computer data authentication, previously referenced [34], should be used to assure accuracy, as well as security, in the transmission of the data. Synchronous transmission is more appropriate with use of computer data authentication.

6.16.7 Control for Vote Summarization

As voting results are received from specific precincts, these data are summarized to provide candidate totals. Validity checks should be used to assure that specific votes are not added twice, or not added to the wrong precinct total, or not added at all. The number of ballots submitted from each precinct, as identified by precinct officials, should be entered into the vote summarizing system and compared against the sum of candidate votes plus overvotes and undervotes tallied for the precinct. Any difference of more than three should trigger a review. (Any difference at all is suspect, but given the current limits of precinct official and ballot reader accuracy, a difference of three may be the minimum practical.)

6.16.8 Vote Reconciliation by Contest

In each vote-for-N contest, whether N is one or any higher integer, the number of candidate votes plus the number of undervotes must equal N times the number of non-overvoted ballots. The number of non-overvoted ballots is the simply the total number of ballots voted for the contest less the number of ballots overvoted for the contest.

6.16.9 Recording of Undervotes and Overvotes

Undervotes and overvotes must be recorded if the vote summarization and reconciliation controls specified above are to be accomplished. The effective use of recounting also depends on the availability of this data. Recording of this data is supportive of GAO standard S1 on Documentation (see section 5.4.5).

6.16.10 Recounting

A manual recount of one percent of the ballots of each contest is recommended. The right of selection of some of the precincts to be recounted should be granted to parties or candidates. The parties and candidates are likely to propose those precincts about whose results they are most suspicious. By recounting those precincts, more confidence in the final results is likely.

Ballots may be recounted on a different, independently managed machine instead of being recounted by hand. Machine recounting permits a larger recount with considerably less effort. If a backup machine is available, and that is recommended as a good management practice, the ballots may be recounted on that machine. Further confidence in the recount may be expected if the management of the backup machine is independent of the organization managing the primary machine and the vote-tallying software is supplied by a different manufacturer. An independent organization could be considered to be one that reports to a different independently elected or appointed official and that receives an independent budget.

An analysis of recounting [105] reveals that for a given level of confidence in the results, more ballots should be recounted as the opposing candidate vote totals become more equal. As the candidate vote totals approach equality, the recount percentage for any confidence level approaches 100%. This result is what one would expect intuitively, and in practice, a full recount is often demanded (if it is not automatic) by at least one candidate when this condition occurs.

The referenced analysis employs the assumption that the number of voters receiving and returning ballots is well-documented, so that frauds or errors involving the addition or subtraction of ballots could not be successfully perpetrated. Any reported result in which the sum of candidate votes (plus overvotes and undervotes) is not equal to the number of ballots submitted can be immediately identified as incorrect. If an erroneous result is reported in which the total of candidate votes plus overvotes and undervotes for a precinct equals the number of ballots submitted for that precinct, the error must be due to a switching of votes between candidates or between a candidate and the overvote or undervote categories. Thus, the complete reconciliation of candidate votes and overvotes and undervotes with ballots cast reduces significantly the possibilities for the reporting of incorrect results.

The referenced analysis shows that if only 1% of the precincts are recounted (the rule in California and Texas, for example), and there are just two opposing candidates who differ by only 1% of the total vote, there is only a probability of .655 (a chance of about two in three) of finding a worst-case error that might be overturning the outcome of an election involving 1000 precincts. For there to be a 99% chance of finding this worst-case error when the candidates differ by 1% of the total vote, 4.3% of the precincts should be recounted, assuming a 1000-precinct situation.

However, the kind of error that is most likely to occur is not the type of deliberate and sophisticated scheme that would require the full percentage recount specified in the analysis in order to be discovered. With a less sophisticated type of error (such as the accidental miscounts in Carroll County, Maryland and Moline, Illinois described respectively in sections 4.1 and 4.8), a smaller recount is sufficient for discovery. The reason that a smaller recount is sufficient with less deliberate errors is that the errors would exist more widely among the precincts, and so a smaller selection of precincts for recounting would be necessary in order to discover the error. Unfortunately, it is not known in advance what kind of error, if any, exists in a reported count.

6.17 Application Internal Controls For DRE Systems

The controls proposed for DRE systems in this section were not included in the 1975 vote-tallying report, as this type of system was only just becoming operational at that time. In the 1975 report, a DRE machine was called a "vote summarizer."

The DRE voting machine presents a special application internal control problem. As discussed in section 3.7.2, a voter-choice set recorded by the machine is not an independent document, as it is created by the machine, not by the voter. The set of votes displayed by the machine for the benefit of the voter during the voting process may not be the set of votes actually used by the machine for summarization and inclusion in the reported results. By design, there can be no independent verification of the operation of the machine. For some, this lack of an audit trail for individual transactions is unacceptable.

Substitute controls for the unavailability of individual voting records should include convincing demonstrations that each DRE machine operated correctly, that is, did not fail, during each voter's use.

6.17.1 Voter Count Match

The number of voters recorded by each machine as having voted should equal the number of voters signed in to vote and assigned to that machine by the precinct officials. That is, records of use of each machine should be individually kept by the precinct officials in order to permit a direct match with the machine records.

6.17.2 Accuracy of Telecommunication of Voting Data

The controls are identical to those for ballot-tallying systems.

6.17.3 Vote Reconciliations

With a record of each undervote (recommended in section 6.10.1), two vote reconciliations are then possible. One reconciliation should demonstrate an equality in the sum of the number of votes and undervotes cast by each voter in all contests. The second reconciliation considers each contest separately, and should demonstrate that the sum of the number of votes and undervotes cast in the contest is consistent with the number of voters who voted for the contest.

First, for every voter using the same ballot style, the sum of the votes and undervotes cast is the same number, equal to the maximum number of votes that could have been cast by a single voter in that ballot style. This simple reconciliation is possible only because overvotes are prevented. A similar reconciliation for ballot-tallying systems is more complex because, in general, overvotes cannot be prevented.

Secondly, for each vote-for-N contest (N may be one or any higher integer), the number of votes for candidates by all voters plus the number of undervotes of all voters should equal N times the number of voters recorded as having voted in the contest.

These reconciliations may be carried out for each individual DRE machine, as well as for groups of machines. The calculation of these reconciliations, and the demonstration of the equalities, should provide added confidence that the DRE machines were performing correctly.

6.17.4 Recounting of Voter-Choice Sets

If the machine-generated voter-choice sets have been recorded on removable storage media, it is an easy matter to recompute the machine-computed vote summaries. It is recommended that this type of recount be carried out for at least 1% of the precincts, using the complete voter-choice data for those precincts. The recount should be carried out on an independently programmed computer for which the removable media can provide data input. As pointed out in section 3.7.2, this recount checks the machine's summarization process, not the machine's recording of the voter's intent.

6.17.5 Post-Election Checkout

Each ballot position on a selected percentage of DRE machines used in an election should be test-voted following the close of polls, to assure that each was working correctly. Selection of some of the machines to be tested should be granted to parties or candidates. If each contest on each machine had only two alternatives, it would be possible to test each ballot position with the casting of just two ballots, assuming no concern for interaction of selections in different contests. As some contests have more alternatives, more than two ballots would need to be cast to check all possibilities.

6.18 The Recommendations In Relation To The Identified Problems

In section 2.9, the problems of computerized vote-tallying were categorized as follows: there is difficulty in verifying reported results (2.9.1), there is the possibility of undiscoverable frauds (2.9.2), and election administrators lack required technical knowledge and resources (2.9.3). The existence of these problems have resulted in a continuing lack of confidence by technically qualified observers in the running of computerized elections.

The most pertinent recommendations that respond to these problems are that the concept of internal control should be extended so as to be applicable to vote-tallying, and that persons knowledgeable in that professional field should be utilized to assist in the establishment of sound operational procedures.

Extension of internal control to vote-tallying requires only the re-definition of the concept of a transaction so that it is applicable to non-financial operations. EDP auditors and internal auditors may be utilized to recommend procedures that assure that results can be verified and that the possibility of undiscoverable frauds is minimized. Specific internal controls applicable to vote-tallying have been provided above. These controls respond to the potential fraudulent manipulations identified in section 2.9.2, and to lack of audit trails and poorly implemented administrative procedures, specified in 2.9.1, (a) and (d).

With the use of the services of knowledgeable professionals in internal control (which includes computer security), and with the efforts of sources of objective technical information (such as the Election Center), election administrators would not be perceived to lack the technical knowledge and resources necessary to overcome problems of computer use that cause unease about reported results. The necessary knowledge required to assure integrity of the vote-tallying process would be available in-house. Thus, administrative errors should be minimized (2.9.3 (a)) and control of the process would not have to be abdicated (2.9.3 (b)). The public would be able to receive assurances that specific threats to system integrity were being adequately handled. Improved confidence should result in reduced risk to vendors entering the market (2.9.3 (d)), and therefore faster introduction of more effective technology (2.9.3 (e)).

Other recommendations have concerned the performance of vote tallying hardware and software, and assurance of their integrity. It is recommended that the specifications developed by the FEC Clearinghouse be considered for adoption by each State when they are issued. The availability of these performance concepts and specifications provides election administrators with additional knowledge and resources that can be used to acquire effectively operating vote-tallying systems. This responds to the concern specified in section 2.9.3 (c).

Tests of logical correctness of vote-tallying software are recommended as part of a certification process, and recommendations are made concerning the treatment of all software to minimize the possibility that operations will be modified fraudulently by hidden code. The implementation of these recommendations should provide additional confidence in the integrity of the systems used to report election results. The certification process, including its tests for logical correctness, responds specifically to the concerns about the design of computer programs and their unavailability to the scrutiny of responsible officials. These concerns were identified in sections 2.9.1 (b) and (c).

REFERENCES

[1] Roy G. Saltman, Effective Use of Computing Technology in Vote-Tallying, National Bureau of Standards, NBSIR 75-687, March, 1975 (available from the National Technical Information Service, Springfield, VA 22161, under order number COM75-11137, and reprinted as NBS Special Publication 500-30, April, 1978, Library of Congress Card Catalog No. 78-5524).

[2] National Clearinghouse on Election Administration, "Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems," drafts, Nov. and Dec., 1987; revised draft expected August, 1988.

[3] National Clearinghouse on Election Administration, "Executive Summary: Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems," draft, July, 1988.

[4] National Clearinghouse on Election Administration, "Implementation Plan, Federal Election Commission Voting Systems Standards Program," draft, Nov. 30, 1987, revised draft expected September, 1988.

[5] National Clearinghouse on Election Administration, "System Escrow Plan, Federal Election Commission Voting System Standards Program," updated Draft, Nov. 30, 1987.

[6] New York Times, "Computerized Systems for Voting Seen as Vulnerable to Tampering," by David Burnham, July 29, 1985, p. 1.

[7] Howard Jay Strauss, "Detailed Explanation of the Questions and Answers," section of enclosure with cover letter to David Burnham, New York Times, Washington, DC, July 22, 1985.

[8] Eric K. Clemons, letter to Mr. Adam Clymer, New York Times, New York, NY, July 23, 1985, p. 2.

[9] New York Times, "Vote by Computer: Some See Problems," by David Burnham, August 21, 1985.

[10] John K. Van de Kamp, Attorney General, letter of transmittal to Hon. March Fong Eu, Sec'y of State, May 30, 1986.

[11] Robert R. Granucci, Deputy Attorney General, Memorandum to Steve White, Chief Assistant Attorney General, "Computer Assisted Vote-Counting - Problems and Recommendations," April 23, 1986, p. 1.

[12] ibid.

[13] San Francisco Examiner, "Ballot computers may not be secure against tampering," by Seth Rosenfeld, Oct. 20, 1986, p. B-1.

[14] Robert L. Lemens, Assistant Attorney General of Texas, Letter to Ms. Karen Gladney, Director of Elections, Election Division, P.O. Box 12887, Austin, Texas 78711, July 15, 1986.

[15] Dallas Morning News, "Texas investigates vote discrepancies, elections in Dallas, state at issue," by Chris Kelley, Sept. 23, 1986, p. 1A.

[16] Dallas Times Herald, "State investigating county vote system," by Scott Sunde and Tim Graham, Sept. 24, 1986, p. A-1.

[17] Myra A. McDaniel, Secretary of State, Voting Systems Security Directive, Austin, TX 78711, Oct. 14, 1986.

[18] Michael Ian Shamos, "Outline of Testimony on Computerized Voting Before the Texas Legislature," Nov. 25, 1986 (copy supplied by Dr. Shamos).

[19] Texas House of Representatives Committee on Elections, Testimony of Nov. 25, 1986 (provided on audio tapes by the office of Rep. Clint Hackney, Chairman); testimony of Suzan N. Kesim.

[20] op. cit., testimony of Anita Rodeheaver.

[21] op. cit., testimony of Tom Eschberger.

[22] Warner Croft, "The Testimony of Warner Croft, Partner in the CPA Firm of Arthur Anderson and Company," Nov. 25, 1986, Texas House of Representatives Hearings of the Committee on Elections (printed copy).

[23] Vernon's Texas Sessions Laws, 70th Legislature - Regular Session, 1987, Chapter 484 (H.B. 1412), pp. 4171-4189.

[24] Joseph P. Harris, Ph. D., Election Administration in the United States, The Brookings Institution, Washington, DC 1934; pp. 17-18.

[25] op. cit., p. 247.

[26] op. cit., pp. 248, 249.

[27] Roy G. Saltman, op. cit., section III.A, p. 10.

[28] ANSI X3.11-1969, *Specification for General Purpose Cards for Information Processing* (revision of ANSI X3.11-1966), American National Standards Institute, 1430 Broadway, New York, NY 10018.

[29] ANSI X3.21-1980, *Rectangular Holes in Twelve-Row Punched Cards*, American National Standards Institute, 1430 Broadway, New York NY 10018.

[30] ANSI X3.26-1980, *Hollerith Punched Card Code* (revision of ANSI X3.26-1970), American National Standards Institute, 1430 Broadway, New York, NY 10018.

[31] Eugene F. Troy, *Security for Dial-Up Lines*, National Bureau of Standards Special Publication 500-137, May, 1986.

[32] William Hetzel, *The Complete Guide To Software Testing*, QED Information Sciences, Wellesley, MA 02181, 1984.

[33] Delores R. Wallace, *An Overview of Computer Software Acceptance Testing*, National Bureau of Standards Special Publication 500-136, February, 1986.

[34] Federal Information Processing Standards Publication 113, *Computer Data Authentication*, National Bureau of Standards, May 30, 1985.

[35] Survey data from Election Data Services, Inc., 1522 K St. N.W., Washington, DC 20005.

[36] *New York Times*, "Texas Looks Into Reports of Vote Fraud," by David Burnham, September 23, 1986, p. A26.

[37] *Carroll Sun* (Westminster, MD), "Human error reversed school board election results," by Steve Kelly, November 18, 1984, p. 2.

[38] Thomas J. Van de Bussche, letter to Dr. Thomas Lewis, President, Carroll County Election Board, November 26, 1984.

[39] Thomas W. Lewis, Thurston E. Ensor, and June S. Gosnell, "Certain Factors Which Involved the Carroll County Board of Election Supervisors, Either Directly or Indirectly, in Producing the Numerical Results of the General Election in Carroll County, November 6th, 1984," December 4, 1984.

[40] Roy G. Saltman, op. cit., section IX.A.6, p. 91.

[41] *Carroll County Times* (Westminster, MD), "Election system under fire nationwide," by Chris Guy, July 11, 1985, p. 1.

[42] Charleston Gazette, "Hutchinson files election complaint," by Fanny Seiler, June 2, 1981.

[43] Charleston Daily Mail, "Miller Indicted, Election Probe Will Continue," by John Luttermoser, Feb. 25, 1982.

[44] Charleston Daily Mail, "Jury Clears Miller of All Charges," by Kay Michael, June 2, 1983, p. 1.

[45] Charleston Daily Mail, "Conspiracy Charged In Election Suit," Feb. 5, 1983.

[46] Charleston Gazette, "Hutchinson charges '80 election fixed, attempts to link Jay's aide," by Fanny Seiler, June 5, 1982.

[47] Charleston Daily Mail, "Amended Lawsuit Filed in 1980 Elections Case," Dec. 3, 1983.

[48] Charleston Daily Mail, "Sour Grapes," May 3, 1985, p. 4A.

[49] Memorandum to The Honorable Mayor and Members of the City Council, "Election Recount in Places 11 and 9," by Robert S. Sloan, City Secretary, April 17, 1985.

[50] Recount Report -- City of Dallas Place 11 and Place 9, April 11, 1985.

[51] Precinct-by-precinct comparison of the number of ballots cast according to the official canvass, April 6, 1987, and the number of ballots cast in the recount, April 11, 1987; data supplied by Mrs. Terry A. Elkins, current address 6050 Northwood Road, Dallas, Texas, 75225.

[52] Terry A. Elkins, Research Findings Concerning the April 6, 1985 Dallas County Joint Election and Testimony to the Texas House of Representatives Committee on Elections of November 25, 1986, photocopy.

[53] Dallas Morning News, "Texas investigates vote discrepancies; Elections in Dallas, state at issue," by Chris Kelley, Sept. 23, 1986, pp. 1A, 4A.

[54] Dallas County Elections Department, "Dallas Morning News Articles (Specific Allegations and Responses)," mimeographed sheet, undated.

[55] Memorandum To Vaughn Duck, "Dallas 4/6/85 Election," by P. J. Lyon, Sept. 18, 1986.

[56] Data supplied by Dallas County Elections Department.

[57] Dallas Morning News, "Dallas County asked to aid vote fraud investigation," March 24, 1987, p. 18 A.

[58] Letter to Mr. Robert L. Lemens, Assistant Attorney General, "Investigation of the 1985 Joint Election in Dallas County," by Theodore P. Steinke, Jr., Assistant District Attorney, Dallas County, October 14, 1987.

[59] U.S. District Court, Northern District of Indiana, South Bend Division, Case No. S83-412, Affidavit of Deloris Jungert Davisson, p. 7, including Emerald Software presentation, pp. 32, 34.

[60] United States District Court, Northern District of Indiana, South Bend Division, Civil No. S83-412, Order of the Court, p. 6.

[61] 788 Federal Reporter, 2d Series, p. 1272: Bodine v. Elkhart County Election Board, 788 F.2d 1270 (7th Cir. 1986).

[62] Atlanta Constitution, "Legislator regains seat in recount," by Susan Laccetti, November 13, 1986, p. 1-A.

[63] Linda Martinson, Britain J. Williams, and Michael L. Witten, "General Election Recount Report, Gwinnett County," November 14, 1987, Georgia Tech Research Institute, Atlanta, Georgia.

[64] State Board of Elections, State of Illinois, Summary of Findings and Observations of State Board of Elections Computer Testing Program, by Michael L. Harty and Ricky S. Fulle, Revised April, 1988.

[65] Washington Post, "Computer Snafu Caught Before Phoenix Election," from Associated Press, Sept. 7, 1986, p. A3.

[66] National Center for Policy Alternatives, Washington, DC, State Report on Election Law Reform, vol. 2, no. 5, pp. 19-22: "Moline election fouled up by computer," by Peter Ellertsen (from Illinois Issues, November, 1985, pp. 12-15).

[67] Oklahoma County Purchasing Department, Report of Engineering Examination and Election Use of the DIMS Precinct Work Station PWS 1000, December 10, 1984 (photocopy).

[68] Oklahoma State Election Board, Rules and Regulations, Section 21-8, "After The Polls Close."

[69] The Sunday Oklahoman, "Security of Elections Described," by Kay Morgan Atkins, January 25, 1987, p. 3-A.

[70] Board of County Commissioners, Oklahoma County, Memorandum to Commissioner Shirley Darrell-Daniels, "Evaluation of Voting Devices," by Kimberly Statum, February 27, 1987.

[71] The Sunday Oklahoman, "Uncertain Vote Count Puzzling to Analysts," by Kay Morgan Atkins, January 25, 1987, p. 1-A.

[72] In the Circuit Court of the Fifteenth Judicial Circuit of Florida, In and For Palm Beach County, Civil Division, Case No. 84-7180 CA(L)H, Complaint, filed Nov. 29, 1984.

[73] Palm Beach Post, "Re-Count Lawsuit Dismissed," March 2, 1985.

[74] In the Circuit Court of the Fifteenth Judicial Circuit of Florida, In and For Palm Beach County, Civil Action Case No. 84-7180 CA(L)H, Amended Complaint, filed Apr. 4, 1985, item 6(i), p. 2.

[75] op. cit.., Defendant Walker's First Requests for Admission To Plaintiff, filed Jan. 22, 1985.

[76] op. cit., Amended Complaint, filed Apr. 4, 1985, item 6(p), p. 3.

[77] op. cit., Amended Motion to Dismiss of Rebecca E. Walker. filed Jan. 16, 1985.

[78] op. cit., Order, by Circuit Court Judge Richard I. Wennet, Sept. 10, 1985.

[79] Salt Lake Tribune, "County Election Computer Fails To Deliver Vote Total on Time," by Dave Jonsson, November 6, 1980, p. B-1.

[80] Election Administration Reports, vol. 16, no. 15, July 21, 1986, "Audit of Recount Detects Error, Restores Stark County, Ohio Commissioner Victor," pp. 2-4.

[81] National Bureau of Standards, Federal Information Processing Standard 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June, 1974.

[82] Roy G. Saltman, op. cit., section V.F.7, p. 53.

[83] Zella G. Ruthberg and Bonnie T. Fisher, Work Priority Scheme for EDP Audit and Computer Security Review, National Bureau of Standards, NBSIR 86-3386, March, 1986, section 1.2, p. 1.

[84] Executive Office of the President, Office of Management and Budget, Circular No. A-123 Revised, "Internal Control Systems", August 16, 1983.

[85] Roy G. Saltman, op. cit., section II.B.2.(c), p. 4.

[86] United States General Accounting Office, Standards For Internal Controls In The Federal Government, 1983.

[87] Stanley D. Halper, Glenn C. Davis, P. Jarlath O'Neil-Dunne, and Pamela R. Pfau, Handbook of EDP Auditing, Warren, Gorham & Lamont, Boston, 1985, Appendix G, p. G-42.

[88] op. cit, Chapter 16, p. 16-11.

[89] op. cit, Chapters 17-19.

[90] Zella G. Ruthberg, Bonnie Fisher-Wright, William E. Perry, et al, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, National Bureau of Standards, Special Publication 500-153, January, 1988, pp. 30, 31.

[91] Roy G. Saltman, op. cit., section II.B.1.(b), p. 4.

[92] op. cit., section II.D.1.(b), p. 7.

[93] op. cit., section II.D.2.(c), p. 7.

[94] The Presidential Commission on the Space Shuttle Challenger Accident, Report to the President, June 6, 1986, Washington, DC, Volume 1, pp. 148, 199.

[95] Roy G. Saltman, op. cit., section II.A.2.(b), p. 3.

[96] op. cit., section VII.A., pp. 78, 79.

[97] op. cit., section VII.B, p. 79.

[98] op. cit., sections V.F.2, V.F.3, pp. 49-51.

[99] op. cit., section VI.C.3, p. 65.

[100] op. cit., section VI.C.4, pp. 65, 66.

[101] op. cit., section IX.G.2, IX.G.3, IX.G.4, p. 98.

[102] op. cit., sections VIII.A, VIII.B, pp. 85, 86.

[103] op. cit., section IX.I.2, p. 100.

[104] op. cit., sections IX.A, IX.B, and IX.D.4, pp. 90-92, 95, 96.

[105] op. cit., Appendix B, pp. 113-122.

[106] Britain J. Williams and Phillip K. Bailey, "An Analysis of the Error Rate in a Punchcard Voting System," Electronics and Computer Systems Laboratory, Georgia Tech Research Institute, Atlanta, Georgia 30332, April 19, 1988.

[107] Lance J. Hoffman, Making Every Vote Count: Security and Reliability of Computerized Vote-Counting Systems, School of Engineering and Applied Science, The George Washington University, Washington, DC 20052, November, 1987.

NBS-114A (REV. 2-80)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET** *(See instructions)*	1. PUBLICATION OR REPORT NO. NBS/SP-500/158	2. Performing Organ. Report No.	3. Publication Date August 1988

4. TITLE AND SUBTITLE

Accuracy, Integrity, and Security in Computerized Vote-Tallying

5. AUTHOR(S)

Roy G. Saltman

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

G87101

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

John and Mary R. Markle Foundation
75 Rockefeller Plaza, Suite 1800
New York, NY 10019-6908

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 88-600573

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

Recommendations are provided to promote accuracy, integrity, and security in computerized vote-tallying, and to improve confidence in the results produced. The recommendations respond to identified problems, and concern software, hardware, operational procedures, and institutional changes.

It is proposed that the concept of internal control, almost universally used to protect operations that produce priced goods or services, be adapted to vote-tallying, a non-priced service. For software, recommendations concern certification, assurance of logical correctness, and protection against contamination by hidden code. For hardware, recommendations concern accuracy of ballot reading, and design and certification of vote-tallying systems that do not use ballots. Improved pre-election testing and partial manual recounting of ballots are recommended operational procedures.

Some recent significant events concerning computerized vote-tallying are reported. These events include development of performance specifications, publication of a series of New York Times articles, and activities in Texas leading to passage of a revised statute on electronic voting systems. Relative vulnerabilities of different types of vote-tallying systems, i.e., punch card, mark-sense, and direct recording electronic, are discussed. Certain recent elections in which difficulties occurred are reviewed, and categories of failures are highlighted.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

accuracy; computer; election; integrity; internal control; public administration; security; vote-tallying.

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

143

15. Price

133

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name ____

Company ____

Address ____

City ________________ State ____________ Zip Code __________

(Notification key N-[illegible])

☆ U.S. GOVERNMENT PRINTING OFFICE: [illegible]— 2 0 1 - 5 9 7 / 9 2 5 5 3

NBS Technical Publications

Periodical

Journal of Research—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Bureau of Standards
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

Stimulating America's Progress
1913-1988

136